Deskundigen adviseren

HACK-TIC

18/19

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN

f8,-



COLOFON

Hack-Tic is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1989. Tics 5/6, 9/10, 11/12, 14/15, 16/17 en 18/19 zijn dubbeldik.
UITGAVE: Met veel moeite door de stichting Hack-Tic. Ook voor al Uw ideale schoonzonen.
ISSN: 0928-0269
MET DANK AAN:: Jansen, The Key, Billsf, Carla, The Dude, Herman Acker, Peter Poelman, Xokum 3, Ing. (Cum Laude), Itarne, Fons, Emmanuel Goldstein, Hanneke, Felipe, Paul, RGB Productions, Vladimir Ulianov, gemeentepolitie Amsterdam, CRI, de 'Stamp-On Stuff-In Mail-Out'-crowd, MAD/MA(C), Wessel, Patrice en Jansen. Verder krijgen we informatie uit de idiootste kringen.
ZWEEP: Carla
ILLUSTRATIES: Koen Hottentot.
HOOFDVERDACHTE:Rop Gonggrijp
C. V.: Archibald Tuttle
KONTAKT: De redaktie is waarschijnlijk nauwelijks te bereiken via postbus 22953, 1100 DL Amsterdam. Internet (UUCP) e-mail: redaktie@hacktic.nl. Tel. 020-6001480, Fax 020-6900968.
PRIJS: Losse nummers kosten 4 gulden en 50 cent, een abonnement voor 10 nummers (of 5 dubbelnummers, net waar we zin in hebben) kost 40 piek. Dit is een dubbelnummer en kost ƒ 8,-. Abonnementsgelden kun je overmaken op gironummer 6065765 t.n.v. de Stichting Hack-Tic. Abonnementen beginnen met het laatst uitgegeven nummer.
INTERNATIONAL RATES: Outside Holland or Belgium, 10 issues cost US$ 35, DM 60. Airmail rates are US$ 50, 80 DM. Payment in cash ONLY to P.O. Box 22953, 1100 DL Amsterdam, The Netherlands. Send e-mail to info@hacktic.nl for more information.
ABONNEMENT VOOR HET LEVEN:
Voor ƒ375,- heb je een levenslang abonnement op Hack-Tic dat zelfs na de dood testamentair op een ander over kan gaan. Het abonnement duurt zolang Hack-Tic duurt. Nooit meer gezeur met het verlengen van je abonnement! Buitenlandse Levens-abos krijgen een gratis woordenboek van Nederlands naar de taal van hun keuze. Als je abonnee voor het leven wordt krijg je alle oude nummers (voor zover voorradig) thuis gestuurd.
PRIVACY: Het is natuurlijk via onze bankafschRiften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld en adres in een enveloppe stoppen en die aan onze postbus (zie 'kontakt') sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale enveloppe, en het abonneebestand is op onze disks versleuteld. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.
DISCLAIMER: De informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt niet noodzakelijkerwijs de mening van de redaktie of uitgever.
NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk wel met bronvermelding) stukken overnemen uit Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.
NABESTELLEN: Oude nummers kosten ƒ4,- en kunnen via de redaktiepostbus besteld worden. Sommige nummers zijn schaars en soms moeilijk te krijgen. Oude nummers worden verstuurd als er een Hack-Tic uitkomt.
HOE: Deze Hack-Tic werd met Ventura 4.0 (onder MS-Windows 3.1) gemaakt op een AT-386 met 4 MB geheugen. De plaatjes werden met een Primax 800 DPI handscanner opgezogen en print-outs van elke pagina werden met een FACIT P6010 lasergeval gezoeft en daarna ambachtelijk gedrukt. Toen hebben we het nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

Hack-Tic 18/19

Er is weer een hoop gebeurd sinds de laatste Hack-Tic. Zo heeft Hack-Tic redaktielid RGB een tijdje bij de gemeentepolitie in Amsterdam gelogeerd. Ook zijn er nogal typische dingen gebeurd met onze telefoonlijnen op het redaktiekantoor. En als die Boeing 500 meter eerder was neergestort was Hack-Tic misschien nooit meer verschenen.

De eerste twee gebeurtenissen in de vorige paragraaf hebben te maken met de komst van grote broer. Harry Onderwater, opperhackervanger van de CRI zegt het in een interview in Penthouse als volgt: "Wat er nu gebeurt is eigenlijk het snoep afpakken van een klein meisje. Jarenlang konden hackers ongestoord van het gestolen snoepgoed genieten. En nu komt ineens de grote broer van het meisje om de hoek kijken die zegt: hé, wat doe jij met mijn zusje. Bam! Het zal gegarandeerd een stuk rustiger worden in hackersland. Daar is het ons om te doen."

Dus pas op: grote broer kijkt naar u. In het interview worden anonieme bronnen bij Binnenlandse Zaken opgevoerd die beweren dat de BVD 10 tot 15 mensen 'op hacking' heeft zitten. Ze zouden zich vooral op de groep rond Hack-Tic concentreren, want "daar immers ontmoeten techno-anarchisten, alternatieve techneuten en techno underground elkaar. Uit binnen- en buitenland. Daar zetelt alle kennis."

Het verslaggeversduo van Penthouse werd volgens eigen zeggen trouwens tijdens een vorige reportage over 'digitale misdaad' al met de bemoeienissen van de BVD geconfronteerd. Zij werden er via een gesprekspartner op het departement van Justitie op attent gemaakt dat hun komst reeds was aangekondigd door de BVD. Hun bron zou toen gezegd hebben: "Jullie hebben waarschijnlijk met een hacker gepraat die, ik durf het bijna niet te zeggen, voor de BVD werkt. Het hoeft niet per se een hacker te zijn, het kan ook een telefoontap zijn geweest."

Onderwater zegt in hetzelfde interview over Hack-Tic: "Een machtig interessant boekje. Gemaakt voor de grote massa. Weet je wat ik wel riskant vind aan Hack-Tic? Het geven van informatie of een handleiding hoe je een systeem moet kraken. Daarmee verschaf je (nog niet kundige) personen een handvat om te beginnen, terwijl Hack-Tic zich niet verantwoordelijk voelt voor de gevolgen. Het staat bijna gelijk aan het geven van de sleutels van een dure sportwagen aan een 17-jarige die twee theorielessen heeft gehad.". Verderop in deze Hack-Tic zitten de sleuteltjes, scheuren maar!

Het lijkt wel of we geen Hack-Tic meer uit kunnen brengen zonder pikante commentaren van overheidsinstanties over ons. Onze PR chef wrijft haar handen.

Het was niet helemaal de bedoeling, maar dit nummer is een beetje een 'paranoia-special' geworden. Op de een of andere manier hadden we ineens een heleboel artikelen die met afluisteren te maken hadden. Nu ik er eens over nadenk.... was dat wel toeval? Normaal verontschuldigen we ons op deze plaats voor de late verschijning. In dit nummer zeggen we gewoon dat het de schuld is van de CIA. In de volgende Tic weer excuses, en hopelijk geen politie-invallen. Safe hacks everyone.

Dan zijn er nog administratieve kleinigheden. Abonnees in Belgie, of in elk ander buitenland, moeten **niet** storten op onze girorekening. Het onderstaande illustreert de gevolgen: de zwendelende afzetters van de Postbank NV jatten dan 11 gulden van ons onder het mom 'transferprovisie', wij krijgen dus maar 29 van de 40 piek. These are the days of lasers in the jungle, maar stop je geld maar gewoon in een envelop als het verder moet dan een paar honderd kilometer. Dat geeft het minste gedoe en het komt tenminste aan. Dus: geen postwissels, geen cheques, geen internationale overschrijvingen, geen andere slimmigheden.

reden van betaling-details of payment

[redacted]

KOTSBANK

muntsoort currency	ontvangen bedrag amount received	koers exchange rate	muntsoort currency	bedrag bij credit amount
NLG	40,00		NLG	40,00
kosten charges			**muntsoort currency**	**bedrag amount**
TRANSFERPROVISIE			NLG	11,00

De beste manier om de Hack-Tic redaktie te bereiken is via electronic-mail (zie colofon). Faxen is een goede tweede. Als je schrijft of belt moet je er rekening mee houden dat het soms erg lang kan duren, als er al iemand terug belt. Het is jammer, maar we hebben per persoon maar twee armen, dus het is niet anders.

PTTers opgelet

Interessante informatie wil vrij zijn

Heb je technische kennis die maar beter niet in handen van het publiek kan vallen? Werk je diep in de buik van het systeem en is het opsturen van informatie naar Hack-Tic je enig overgebleven uiting van verzet? Hack-Tic publiceert voor een techno-enthousiast publiek dat de schoonheid van het telefoonnet nog weet te waarderen. Dus zet op flop en in een envelop!

We zijn vooral op zoek naar interessante informatie die eens een saai leven leidde binnen PTT-Telecom. Software voor centrales, manuals voor LOPAS, WERKNET, 5ESS, BRIT, en de 06 en 09 centrales, we noemen maar wat. Hele gewone zaken als een intern telefoonboek worden hier hoog gewaardeerd.

Natuurlijk, als je baas er achter komt wordt je ontslagen, maar zeg nou zelf, maakt dat het leven niet een beetje spannend?

Beveiliging op het ethernet

Nachtmerries van valse pakketjes en gatenkaas uit Provo

N*etwerk*. Een populairder modewoord is in het automatiseringsjargon van vandaag niet te vinden. Er zijn een hoop verschillende manieren om computers aan elkaar te koppelen. Een van de meest gebruikte methoden heet *ethernet*. In een ethernet zijn alle computers door middel van een coaxkabel met elkaar verbonden. Met een snelheid van 10 miljoen bits per seconde kan elke computer (vaak door middel van een speciale kaart) communiceren met alle anderen.

Er kan slechts één computer tegelijk aan het woord zijn, en dus wordt alle data opgesplitst in kleine pakketjes, die één voor één op de kabel worden uitgezonden. Iedere op het net aangesloten computer 'ziet' alle pakketjes voorbijdobberen, maar alleen de geadresseerde pikt het pakketje van het net. De beveiliging van ethernet is er dus op gebaseerd dat niemand vals speelt. Ethernet is ontwikkeld voor gebruik in universiteiten en onderzoekscentra en is nooit bedoeld om een veilig netwerk te zijn.

Een aantal netwerkmakers zag een gat in de markt van kantoren en bedrijven. Onder hen ook de huidige marktleider Novell uit Provo in de Amerikaanse staat Utah. Zij ontwikkelden Novell Netware, een stuk software om een PC te gebruiken als file-server, die alle andere PC's op een kantoor van één hard disk gebruik laat maken. Netware kan voor de feitelijke verbindingen tussen de computers gebruik maken van een hoop netwerken waaronder ethernet. Ethernet is goedkoop en snel en dus dè oplossing voor alle automatiseringsproblemen. Novell Netware heeft wachtwoorden én een uitgebreid systeem van file-privileges, dus met de beveiliging zit het wel goed. Edoch, iemand is de klanten vergeten te vertellen dat al die mooie 'veilige' software voor het datatransport afhankelijk is van een netwerk dat *alle* data bij *alle* computers in het gebouw aflevert.

Ethernet

Elke ethernetkaart heeft zijn eigen unieke adres, van 6 bytes lang. De eerste 3 bytes geven aan van welke fabrikant de kaart is. Als een van de aangesloten computers iets wil melden aan een van de andere computers, dan stuurt hij een pakketje met data over het netwerk met daarin het adres van de computer waarvoor deze data bestemd is, gevolgd door het adres van zijn eigen netwerkkaart. Het adres dat de kaart aan het netwerk doorgeeft als afzender kan bij veel kaarten software-matig ingesteld worden. In principe kan elke ethernetkaart zich dus voordoen als elke andere kaart. Normaal gesproken geeft alleen de 'geadresseerde' dit pakketje door aan zijn operating system, maar de meeste kaarten bieden de mogelijkheid om aan te geven in welke mate data van het netwerk dient te worden door gelaten. De

mode waarin elk pakketje van het net geplukt wordt heet de 'promiscuous mode'.

In de ethernetpakketjes ligt vaak een pakket van een hoger protocol 'ingepakt'. In een UNIX omgeving worden TCP/IP pakketjes in ethernetpakketjes gestopt, bij Novell netwerken zijn het IPX-pakketjes die over het netwerk zoeven, ook weer veilig ingepakt in de ethernetpakketjes. In de 'header' van deze TCP/IP of IPX pakketjes zit weer een geadresseerde en een afzender.

In een IP netwerk gaan de passwords ongecodeerd over de ether. Heb je dus fysieke toegang tot het netwerk, of heb je voldoende bevoegdheden op één van de aangesloten machines, dan is het geen probleem om in elke aangesloten computer binnen te komen. Er zijn diverse programma's in omloop die het vergaren van interessante data van het netwerk wat makkelijker maken:

- *Gobbler*, voor de PC, op het Internet verkrijgbaar via anonymous ftp van dutepp0.et.tudelft.nl
- *tcpdump*, voor het bekijken van TCP/IP paketten op unix, verkrijgbaar via anonymous ftp van elke grote ftp site

Beide programma's staan overigens ook op het hacker-BBS *Utopia* in Amsterdam. Het is dus niet de bedoeling om met deze programma's in een UNIX-netwerk op zoek te gaan naar TCP/IP packets bestemd voor port 21 of 513. Hierin staan namelijk nogal eens logins en de bijbehorende passwords om de betreffende unix in te komen. Port 21 is het poortnummer waarover een ftp (File Transfer Protocol) verbinding wordt opgebouwd, port 513 is de poort die gebruikt wordt door rlogin.

Novell

Bij Novell netwerken gaan de passwords gecrypt over het netwerk. Op de server worden de passwords bijgehouden in de 'bindery', deze is te vinden in SYS:SYSTEM, als net$obj.sys, net$prop.sys en net$val.sys. Alleen de server kan de passwords lezen, bovendien zijn de passwords versleuteld opgeslagen. De inlogprocedure gaat als volgt:

1. Het werkstation versleutelt het password met het userID, met als resultaat een code van 16 bytes.
2. het werkstation vraagt aan de server een 'logkey', dit zijn 8 min of meer willekeurig gegenereerde bytes.
3. met deze logkey versleutelt het werkstation het al versleutelde password nog een keer, met als resultaat 8 nieuwe bytes
4. deze 8 bytes worden samen met de username aan de server gestuurd
5. de server voert stap 3 ook uit, en vergelijkt het in stap 4 opgestuurde resultaat met zijn eigen resultaat. Als deze overeenkomen wordt aangenomen dat het correcte password is ingevoerd.

De Novell login-procedure

De server kijkt overigens eerst of het password toevallig een null password is. In dat geval wordt de inlogpoging niet geregistreerd. LOGIN.EXE probeert eerst één keer met een NULL password in te loggen, daarna vraagt het om een password, waarmee vervolgens ook wordt geprobeerd in te loggen. Hiermee wordt voorkomen dat een gebruiker die geen password heeft wel om een password gevraagd wordt. De server vat inloggen zonder password dan ook niet op als een login-fout..

De bug in Novell versies ouder dan 3.11 / 2.2 waardoor je na een groot aantal inlogpogingen toch werd toegelaten, zat 'm in de generatie van de logkey. Deze bestaat soms uit 2 keer de zelfde 4 bytes, wat tot gevolg heeft dat de uitkomst van stap 3 altijd een rij van 8 nullen is, ongeacht het password. Mijn patch KNOCK.EXE uit de vorige Tic maakte hiervan gebruik, door gewoon net zo lang te proberen tot de server de deur opendoet.

Door de packets met de logkeys, en de packets met de versleutelde passwords op te vangen, krijg je in principe genoeg informatie om vervolgens op dezelfde manier als bij UNIX passwords een password-hacker te gaan gebruiken.

Je kunt de passwords dan off-line gaan kraken. Het algoritme dat Novell gebruikt om passwords te versleutelen is zelfs veel sneller dan het gewijzigde DES algoritme dat bij UNIX gebruikt wordt. Je begrijpt dat Novell niet blij was met de publicatie van deze fout (ze waren zelf al een tijdje op de hoogte). In de nieuwste versies van Novell Netware is het gat gedicht, en voor de oudere versies is een patch beschikbaar om het gat te dichten. Niet dat iemand die geinstalleerd heeft... Het beveiligingsgat waarover de een paar weken geleden nogal wat in de kranten heeft gestaan, heeft echter niets met deze bug te maken, maar met het eerder genoemde meeluisteren (en meepraten) op het net.

```
ethernet header
    - destination ethernet adres : 6 bytes
    - source ethernet adres : 6 bytes
    - packet lengte : 2 bytes
IPX header
    - checksum : 2 bytes,  wordt nooit gebruikt
    - lengte : 2 bytes
    - transport control : 1 byte
    - packet type : 1 byte  11 hex = server functions
    - source ipx adres
    - destination ipx adres
novell header
    - type : 2 bytes, 2222= packet van PC naar server,
                      3333=server - PC
    - sequence number : 1 byte
    - connection nr : 1 byte
    - ???? : 2 bytes
    - function : 1 byte, 17=bindery control, 34=file functions ...
data
```

Structuur van een Novell pakketje

Veel systeembeheerders zullen het niet op prijs stellen als je naar het netwerk gaat 'luisteren'. Ook willen ze niet dat je de packets die van de PC van de systeembeheerder af komen gaat bekijken. Let bijvoorbeeld niet op het het laatst gestuurde packet met ipx type 11, hoog daarna niet het sequence nummer op, geef het niet een leuke functie mee, bijvoorbeeld in het bijzonder niet:

```
  novellheader : functie 17h
41                        : bindery functie : add object to set
25                        : lengte van data
0001-0A:"SUPERVISOR":  type-length:"naam"  van toe te voegen object
0F:"SECURITY_EQUALS": property naam
0001-05:"GUEST"       : van gebruiker GUEST
```

Pas Op: Dit nooit op het ethernet uitzenden!



Stuur je een aldus gevormd packet toch naar de server, en heb je je eigen ethernet adres veranderd in dat van de systeembeheerder, dan zou namelijk het guest account supervisor rechten krijgen, en dat kan niet de bedoeling zijn. Gelukkig zijn er ethernet kaarten die je voor al dit soort onheil behoeden. Je kunt de kaart dan namelijk niet zodanig programmeren dat hij elk packet op het netwerk opvangt, zodat je niet kunt zien wat het huidige sequence-nummer is van de systeembeheerder. De enige manier om de bovenstaande subversieve aktiviteiten uit te voeren is dan om gewoon elk sequence nummer te proberen.

Gelukkig heeft Novell daar iets op gevonden. Ze hebben namelijk een patch uitgebracht, die verbindingen verbreekt op het moment dat er een verkeerd sequence nummer wordt gedetecteerd. Alleen is het wel jammer voor je systeembeheerder, die dan ook wordt uitgelogd. Ook na netwerk-errors (en die komen nog al eens voor) wordt je uitgelogd. Je moet wat over hebben voor de 'veiligheid' op je netwerk.

Voor iedereen die zijn belangrijke en vooral geheime gegevens aan een Novell netwerk, of elk ander ethernetgebaseerd netwerk heeft toevertrouwd: vannacht weer lekker slapen.

Itsme

Homevox Security Code!

Er zijn diverse kleine centrales op de markt voor huis-, tuin- en keukengebruik. Wie een Homevox van PTT Telecom koopt waant zich veilig. Hij krijgt niet zomaar alleen een veel te dure, officieel goedgekeurde merkcentrale van grote broers eigen Taiwanese leverancier in handen. Voor die 50% extra koopt hij ook het beroemde PTT veiligheidsgevoel mee. Je weet wel, van die verdelerkasten waar iedereen naar hartelust op jouw kosten kan bellen, die gepeperde rekeningen die geen tegenspraak dulden en die toestellen die graag dienst doen als verborgen microfoon.

Met de Homevox wordt deze traditie van dienstverlening met een staartje aardig voortgezet. Want de Homevox komt met een ingebouwde beveiliging. Door middel van een zelf in te stellen PIN kan de eigenaar zich namelijk beschermen tegen onbevoegd gebruik van zijn lijn.

Wel wordt hem aangeraden zijn kist ergens te monteren waar onbevoegden niet makkelijk bij kunnen komen. Niet zozeer uit vrees dat ze de draadjes omzetten. Nee, dat niet. Eerder vanwege het feit dat de PIN terugvalt naar de default als de stroom even uitgaat. Onbevoegden mogen dus niet aan de stroomkabel kunnen komen. Aldus de handleiding.

Kennelijk denkt de PTT niet aan het even uitdraaien van de zekering. Of misschien toch wel. Angstvallig wordt de klant ook aangeraden het 'geheime' deel van de handleiding veilig op te bergen. Daar staat namelijk de default PIN in gemeld: 7373. Deze is voor alle Homevoxen hetzelfde, dat moet je dus niet onder ogen van vreemden laten komen.

Van een battery-backup hebben ze bij PTT Telecom blijkbaar nog niet gehoord. Waarom die moeite nemen voor klanten die toch niet beter weten? Klanten zijn er toch om zoveel mogelijk verneukt te worden? Zoals die lachwekkende oudjes die werkelijk dachten voor minder dan 5 minuten te betalen als ze minder dan 5 minuten belden?

Maar dat maakt allemaal niets uit. De koper van deze waardeloze beveiliging krijgt er een waardeloos gevoel van zekerheid bij, en daar gaat het om. Tegenwoordig heet dat marketing.

Vladimir Ulianov

```
14CD:0100 B80102        MOV     AX,0201
14CD:0103 B90100        MOV CX,0001
14CD:0106 BA8000        MOV DX,0080
14CD:0109 0E            PUSH    CS
14CD:010A 07            POP ES
14CD:010B BB0006        MOV BX,0600
14CD:010E CD13          INT 13
14CD:0110 BEBE07        MOV SI,07BE
14CD:0113 8B8448FE      MOV AX,[SI+FE48]
14CD:0117 B92000        MOV CX,0020
14CD:011A D1C0          ROL AX,1
14CD:011C D1C0          ROL AX,1
14CD:011E D1C0          ROL AX,1
14CD:0120 05A35C        ADD AX,5CA3
14CD:0123 3104          XOR [SI],AX
14CD:0125 46            INC SI
14CD:0126 46            INC SI
14CD:0127 E2F1          LOOP    011A
14CD:0129 B80103        MOV AX,0301
14CD:012C BB0006        MOV BX,0600
14CD:012F B90100        MOV CX,0001
14CD:0132 CD13          INT 13
14CD:0134 803E3D0600    CMP BYTE PTR [063D],00
14CD:0139 7212          JB  014D
14CD:013B 8B0E3E06      MOV CX,[063E]
14CD:013F 8B164006      MOV DX,[0640]
14CD:0143 B8010A        MOV AX,0A01
14CD:0146 CD13          INT 13
14CD:0148 B80103        MOV AX,0301
14CD:014B CD13          INT 13
14CD:014D CD20          INT 20
```

PC-Lock hack-utility, zie pag. 11

How to hack PC-Lock.

PC-Lock Disk Protection System is een produkt van Johnson Computer Systems Inc. PC-Lock pretendeert je harddisk te kunnen beveiligen tegen ongewenst gebruik. Dit soort uitspraken doet het bloed van de rechtgeaarde hacker natuurlijk kriebelen. Voor deze gelegenheid heb ik versie 2.3 eens onder de loep genomen.

Iets meer over PC-Lock

PC-Lock kun je installeren met of zonder system administrator password. In het eerste geval kun je ook nog vier user passwords instellen. Verder is het mogelijk PC-Lock te installeren met een high security option (/HS). (Dit om het hackers *nog* moeilijker te maken). Als je boot vanaf je harddisk vraagt PC-Lock je om een password. Het is ook mogelijk om van floppy te booten, en met behulp van het bijgeleverde programma Unlock je harddisk aan te spreken. Bij het opstarten van Unlock wordt je (uiteraard) ook om een password gevraagd.

Hoe gebeurt het

PC-Lock versleutelt de partition table van je harddisk, om te voorkomen dat je vanaf floppy boot, en vervolgens je harddisk gewoon kan gebruiken. Het essentiele deel van PC-Lock verstopt zichzelf in het hoofd-boot-record (kant 0, spoor 0, sector 1) van je harddisk, en kan de versleutelde partition table weer leesbaar maken. Dit gebeurt door middel van een lullig algoritmetje (XOR-instrukties). Dit algoritme is zijn eigen inverse, dus je kunt het ook gebruiken om de partition table weer in zijn oorspronkelijke (versleutelde) staat terug te brengen. Als PC-Lock geinstalleerd is met de /HS optie, is de ECC van de eerste sector van je root directory door PC-Lock veranderd. Deze ECC is een Error Correcting Code van vier bytes, en kan gelezen worden met int 13h, funktie 0Ah. Dit is wat PC-Lock doet, en vervolgens wordt deze sector op de normale manier teruggeschreven, zodat er nu een correcte ECC toegevoegd wordt. Volgens de officiele documentatie kan deze funktie (int 13h, funktie 0Ah) alleen door AT's uitgevoerd worden. Dit blijkt flauwekul te zijn.

De hack-utility

Het bijgevoegde programma voert bovenstaande funkties netjes voor je uit. Het controleert ook of PC-Lock met /HS optie is geinstalleerd, en heft ook deze beveiliging op. Je hoeft het alleen nog maar zelf in te typen :). Dit gaat het makkelijkst met debug. Maak er dan een .COM bestand van.

De procedure is als volgt: boot van flop, run je hack-util en reboot van flop. Nu kun je gewoon gebruik maken van de harddisk. Een leuke bijkomstigheid is dat je nu ook system administrator rechten hebt. Het algoritme gaat er overigens wel vanuit dat de beveiligde harddisk drive C: is. Als dit niet zo is moet je regel 106 even aanpassen.

Als je PC-Lock niet wilt verneuken, en de beveiliging intakt wilt laten, moet je nu nogmaals je hack-util draaien. De partition table is nu weer versleuteld, maar je kunt de harddisk gewoon gebruiken.

Nog een bugje..

Als je een user password hebt, maar je zit in een vervelend login-script waar je uit wilt, is het leuk om te weten dat ctrl-c en ctrl-break weliswaar onderschept worden, maar dat alt-3 nog gewoon werkt... Overigens werkt ctrl-c ook, als je hem maar geeft voordat de autoexec.bat loopt. Knullig!

Succes d'r mee en have phun...

Fons

Je kunt in de schimmenwereld van de computer underground je kont niet keren of je stoot op lieden die ten stelligste beweren dat hun telefoon toch minstens door wel vijf instanties wordt afgeluisterd. Bewijzen? "Nadat ik met X over de telefoon over Y had gesproken heb ik die blauwe mercedes wel drie keer langs zien rijden." Paranoia rules. Hack-Tic schaart zich in de rij van organisaties en personen die zichzelf belangrijk genoeg vindt voor een eigen telefoontap.

Hack-Tic afgeluisterd?

Het verhaal begint op vrijdag 12 juni 1992. Een computer aan het lokale netwerk hier op het Hack-Tic hoofdkwartier wilde geen modemkontakt meer opnemen met 'sun4nl', een computer van de organisatie 'nlnet' die ons vier keer per dag van electronic mail en nieuwsberichten voorziet. Ook de andere computers in het Hack-Tic Netwerk, die via onze computer van dezelfde diensten gebruik maken, konden geen kontakt meer met ons krijgen.

Ik probeerde handmatig kontakt te maken met 'sun4nl'. Ons modem pakte keurig de lijn op, maar in plaats van een kiestoon klonk een schelle, hoge piep uit het luidsprekertje. Ik startte het communicatieprogramma Telix en tikte 'ATDT' direct naar het modem. Dezelfde pieptoon. Klotemodem. Dit high-speed modem, waarmee je snelheden van 14400 bits per seconde over de telefoonlijn kunt pompen, hadden we nog niet zo lang. Hoewel het best aardig werkte waren we er niet zo heel blij mee, want als je de datacompressie aanzette hing het nog al eens.

3000 Hz pieptoon

De volgende dag kwamen Felipe en Paul langs om naar het modem te kijken. Felipe en Paul zijn samen het 'Hack-Tic Netwerk Troubleshooting Team'. Zodra iets ingewikkeld wordt komen ze langs om het allemaal in orde te maken. Ze hadden twee andere high-speed modems mee om te bevestigen dat het kapotte modem echt het enige probleem was. Modem nummer 1 werd aangesloten en getest. Weer die pieptoon.

We keken elkaar wat vertwijfeld aan en langzaam kroop de gedachte naar boven dat het wel eens niet ons modem kon zijn, maar de prachtige machinerie bij het voormalig staatsbedrijf. Die digitale wondermachine, die zowaar in staat was om DTMF-tonen te herkennen, zond ons een pieptoon.

Bill (onze telefoontechnicus bij uitstek, u kent hem van zijn artikelen in dit tijdschrift) zette snel zijn New-York Telephone test-set op de lijn en concludeerde dat de lijn ook in opgehangen toestand nog steeds die pieptoon gaf. Je kunt met zo'n test-set namelijk ook luisteren naar een lijn zonder zelf op te nemen. Verder kwam hij erachter dat je als je opnam wel degelijk een kiestoon kreeg. Die hadden we gewoon niet gehoord omdat ie overstemd werd door die pieptoon; een modemspeakertje levert nou eenmaal geen hifi-kwaliteit.

Met behulp van de Demon-Dialer werd snel vastgesteld dat het hier ging om een toon van precies 3000 Hz. Vooral het feit dat de toon ontzettend

Vooral het feit dat de toon ontzettend stabiel was wees erop dat hij waarschijnlijk met een kristal werd gegenereerd. Dit sloot toevallige oscillaties uit. Hoewel we zeker wisten dat er geen andere zaken aan die lijn hingen zijn we toen voor een laatste test naar de meterkast gegaan. Hier hebben we alles wat zich binnenshuis bevond losgeschroefd van het PTT-net. Bij het inprikken van de testtelefoon was weer de pieptoon te horen.

Wat het ook was, het kwam zeker niet bij ons vandaan. Die zaterdagavond werd het probleem gemeld bij de storingsdienst van PTT-Telecom en daarmee was de kous af, dachten wij.

Zondag was de pieptoon er nog steeds (de PTT repareert alleen in het weekend als je een grote klant bent die één van hun centrales wil kopen). Terwijl Bill kontroleerde of de toon er nog was door even te luisteren aan de test-set die we nog steeds aan die lijn hadden hangen, greep ik een andere lijn om een uitgaand gesprek te maken naar Felipe.

Bill's gezichtsuitdrukking doorliep in een paar seconden een hele reeks emoties. Uiteindelijk sprak hij: "Hmmmm..... Ehrrrr.... Pfah......". Toen ik hem nogal vragend aankeek voegde hij er aan toe: "Hgggggggnaaah".

Ik vroeg Felipe om even aan de lijn te blijven. Bill begon uit te leggen dat de 3000 Hz toon weg was en dat hij mijn stem en die van Felipe 'geinverteerd' hoorde. Ik vroeg Nils (die ook wat rondhing, het wil nog wel eens druk zijn hier) om even met Felipe te praten terwijl ik de test-set van Bill overnam.

Geen twijfel mogelijk, vervormde stemgeluiden.

stemvervorming

Een van de eenvoudigste manieren om iemands stem te vervormen is om de spraak te 'inverteren'. Het werkt als volgt. Je neemt een toon en trekt het te vervormen stemgeluid er van af. Meer technisch: Je singlesideband moduleert de spraak op de toon.

De politie gebruikt de bovenstaande methode nogal regelmatig voor het radioverkeer dat niet echt geheim is, maar wat ook weer niet iedereen hoeft mee te luisteren. Ze noemen het 'scramble'. Iedere echte scannerfreak heeft dus een apparaatje in z'n scanner gebouwd om de spraak weer terug te draaien. Een schemaatje voor iets dergelijks vind je elders in deze Tic.

Het inverteren van geluid mag dan iets heel simpels zijn, het gebeurt niet zomaar, er komt (in ieder geval bij laagfrequente signalen zoals spraak) apparatuur bij kijken.

Er zou theoretisch een hoop mis kunnen gaan in een telefoonsysteem dat een pieptoon zou kunnen verklaren. Een spraakinversie van de ene naar de andere lijn is een heel ander verhaal. Zeker als je je bedenkt dat de betreffende twee lijnen niet op dezelfde centrale zitten. Onze datalijn is aangesloten op een supermoderne AXE centrale van Ericsson, onze spraaklijn zit op een PRX-A (een computergestuurde reedrelais centrale).

We hebben de rest van die zondag alternatieven proberen te bedenken voor de conclusie dat iemand iets aan onze lijn had gehangen dat er niet thuishoorde. En als je er vanuit gaat dat het de bedoeling was dat we het niet zouden merken, dan hadden ze een nogal stomme fout gemaakt.

Social Engineering

Ik besloot dat het tijd was om mijn Social Engineering vaardigheden in de strijd te werpen die ik al jaren niet meer

is mijn aktieve hack/phreak carriere er namelijk min of meer volledig bij ingeschoten.

Die maandag (15 juni) belde ik naar het hoofdnummer van PTT Telecom in Amsterdam en vroeg ik naar het nummer van de hoofdverdeler in Diemen. De hoofdverdeler is niets meer dan een immens kabelrek waar alle lijnen van een bepaald gebied binnenkomen en over de centrales verdeeld worden. Al onze lijnen lopen over de hoofdverdeler in Diemen.

De telefoon op toestel 2018 (020-6742018 van buitenaf) werd beantwoord door Fred. Ik vertelde dat ik een onderhoudsmonteur was (ik gebruikte alleen mijn voornaam, dat doen ze bijna allemaal bij de PTT) en dat ik nu bij een abonnee zat met een vreemd probleem. Ik legde uit van de piep op de lijn. Ik was niet de eerste die hem hiervan vertelde. Hij had zelfs al een telefoontje gehad van een andere monteur die met ditzelfde geval bezig was. "Dat is ook de eerste keer, dat jullie van buitendienst met zoveel mensen aan iets bezig zijn". Hij legde uit dat de lijn opnieuw bedraad was met kleurcode 2, een code die men normaal niet gebruikt in die verdeler. Zijn doormeet-apparaat gaf aan dat de draad van en naar de centrale contact maakte, maar er was een andere kleur draad gebruikt.

Ik vroeg hem de draad te volgen, en dat deed hij prompt. Onze lijnen zaten op een rek dat hij nog nooit eerder had gezien. Op mijn aandringen leerde nader onderzoek dat op dat rek alle draden zaten naar elders in het gebouw. Aangezien het mij duidelijk was dat mijn telefoon zich niet in het gebouw van de hoofdverdeler in Diemen bevond vroeg ik hem om deze extra draad gewoon door te knippen. Zijn instructies waren echter om niet aan draden te zitten als hij de kleurcode waarmee ze waren vastgezet niet kende. Ik kon hem niet overhalen en dus legde ik maar neer, ik wist immers genoeg.

Ik heb Fred iets later nog een keertje terug gebeld en open kaart met hem gespeeld. Ik vertelde van Hack-Tic en onze artikelen over internationaal telefoneren, gratis bellen in cellen en zo meer. Ik vertelde hem ook wat ik dacht van die pieptoon op mijn lijn. Hij hoorde mijn theorie aan en zei dat hij dat niet kon bevestigen, en ook niet kon ontkennen. Toen ik vroeg of hij wel vaker lijnen met een kleurcode 2 zag brak hij het



'ACHTER AANSLUITEN, VRIEND!'

gesprek af. "Je lijn wordt gefikst, ik zou maar gewoon afwachten". Ik stelde duidelijk een vraag die hij niet mocht beantwoorden.

Toen we de brievenbus leeghaalden bleek er die ochtend een monteur langs te zijn geweest. Nou liggen alle hackers 's ochtends nog lekker op 1 oor, en dus.... Ik maakte telefonisch een nieuwe afspraak voor de volgende dag.

Dinsdagmorgen arriveerde de man van de PTT. Hij zei te geloven dat het probleem "ergens tussen de centrale en ons" zat. In zekere zin waar: de hoofdverdeler voldoet aan die beschrijving. Ik wilde gewoon die lijn terug en besloot dus niet tegen te spreken. Hij greep een draagbare autotelefoon uit zijn zak en belde met één van zijn maatjes. Samen zetten ze onze datalijn op een hele nieuwe draad van hoofdverdeler naar mij. Weg pieptoon.

Telefoontap

Stel: Iemand probeerde ons af te luisteren. Bij het aansluiten van de nieuwe datalijn heeft men een foutje gemaakt: onze spraaklijn was aangesloten op het punt waar normaal de lijn zit die het geluid naar de afluisterende persoon of instantie brengt. Wij hoorden dus het signaal dat naar de tapkamer had gemoeten. Op die lijn is het signaal met 3000 Hz geïnverteerd om te voorkomen dat iedere PTTer mee kan luisteren met getapte gesprekken. Verder wordt de 3000 Hz toon op de lijn gezet als de hoorn op de haak ligt om aan te geven dat de recorder gestopt kan worden.

Als dit een echte poging was om ons te tappen dan zouden ze dus de in- en uitgang van het circuit dat voor onze data-lijn bedoeld was wel op de twee lijnen naar de aftappende instantie hebben gehangen.

Big Brother

Als je een tijdschrift als Hack-Tic uitgeeft is het niet zo vergezocht om er van uit te gaan dat in ieder geval een deel van je telefoonlijnen soms wordt afgeluisterd. Het is nu al weer een tijdje geleden, maar een hoop vragen blijven hangen. Was dit een illegale tap? Was dit de PTT zelf die wel eens wilde weten waar we precies mee bezig waren? Als het een legale tap was, waar worden we dan van verdacht?

Hoe dan ook: het Hack-Tic Netwerk was twee dagen onbereikbaar, en dat zat me nogal dwars. Ik ben niet paranoide, en ik wil het ook helemaal niet zijn. Zo sta ik nog steeds open voor elke andere verklaring van het bovenstaande. Het is immers totaal belachelijk dat de lijnen van een openbaar verschijnend tijdschrift worden afgeluisterd. Als we criminelen waren die iets verborgen hadden willen houden dan waren we geen tijdschrift begonnen. Dat wil niet zeggen dat we helemaal geen geheimen hebben: veel van onze schrijvers kiezen ervoor om onder een pseudoniem te publiceren en veel van onze bronnen willen alleen met ons praten onder garantie van anonimiteit.

Hun bescherming staat of valt met een overheid die zich aan de spelregels houdt. Een overheid die haar eigen wetten breekt mag ook niet verwachten dat anderen zich er aan houden.

Rop

Internet Relay Chat (IRC)

IRC staat voor Internet Relay Chat. De naam zegt het eigenlijk al: IRC is een chat netwerk op het Internet, het grote netwerk dat tienduizenden, hoofdzakelijk academische, computers over de hele wereld met elkaar verbindt. IRC is voor de directe communicatie, wat UseNet news is voor het berichtenverkeer: een snelle methode om met veel mensen met een zelfde interesse te communiceren.

Nu bestaat er al jaren 'talk'. Talk is het on-line equivalent van 'mail'. Het maakt het mogelijk om met iemand anders op het internet een 'one-to-one chat' te hebben. 'talk' heeft echter veel tekortkomingen, zo kun je bijvoorbeeld maar met 1 ander persoon chatten. IRC is gebouwd op dit principe, maar heeft veel meer mogelijkheden. Het is via IRC mogelijk om met meerdere mensen van over de hele wereld tegelijkertijd te praten.

Omdat er op IRC honderden mensen tegelijk aanwezig zijn, was het nodig om er voor te zorgen dat niet iedereen de uitvoer van alle anderen onder zijn neus krijgt. Daarom bestaat IRC uit 'channels'. Ieder channel heeft een eigen topic. Zo zijn er channels als #amiga, #warez, #hottub en natuurlijk #hack. Binnen zo'n kanaal zijn dan meestal een paar mensen over dat specifieke onderwerp aan het praten. Toen ik dit artikel schreef waren er 685 users op IRC, verdeeld over 238 channels. Zoals je ziet, behoorlijk druk.

Hoe werkt IRC nu precies? IRC is gebaseerd op het client-server principe. Over de hele wereld draaien servers. De servers staan via een netwerk boomstructuur met elkaar in verbinding. Om op het netwerk te komen, moet je een client programma opstarten. Dit programma maakt een connectie met een door jou opgegeven server. Het beste is het om een server te kiezen die in netwerk-opzicht het dichtst bij ligt. Ieder bericht of commando dat je dan verstuurt wordt van server tot server doorgegeven, todat het op de plaats van bestemming is. Er zijn op dit moment clients beschikbaar voor alle gangbare unix systemen, VAX/VMS, MS/DOS, Apple-Mac en waarschijnlijk voor nog veel meer systemen.

Om op IRC te komen hoef je dus alleen de client-software te hebben op een computer die aan het Internet hangt. Je moet aan deze client opgeven van welke server hij gebruik moet maken. Veel nederlandse computersystemen die op het Internet aangesloten zijn hebben inmiddels al een client op het systeem staan. Ga voordat je zelf een client gaat installeren dus eerst eens na of er misschien al een is. Als je gebruik maakt van een legaal account is het misschien een goed idee om even met het systeembeheer te overleggen.

Het is onmogelijk om hier alles over IRC uit te leggen. IRC omvat tientallen commando's. Als je meer over IRC wilt weten, is het beste gewoon inloggen en proberen. IRC heeft een ingebouwde help functie (/help) die voor de meeste mensen genoeg informatie geeft. Verder zijn er nieuwsgroepen, alt.irc en alt.irc.ircii, die meer informatie geven. Als dat alles niet genoeg is, kun je altijd even een mailtje sturen naar bosman@fwi.uva.nl en zal ik proberen te helpen.

Hier kun je uit de genoemde directories client software ophalen met anonymous-ftp.

```
cs.bu.edu          irc/clients
nic.funet.fi       pub/unix/irc
coombs.anu.edu.au  pub/irc
```

En dit zijn wat servers waarmee je je client zou kunnen verbinden. Voor Nederland is de server in Delft waarschijnlijk het beste.

```
svbs01.bs.win.tue.nl    ircserver.et.tudelft.nl      nic.funet.fi
```

scorpio

In de vroege morgen van woensdag 6 mei 1992 stond 12 man politie op de stoep van onze redakteur RGB. Zijn relaas:



De Inval

Ik heb een tijdje samen met een vriend een bedrijfje gehad dat PC's verkocht. Op die bewuste woensdag word ik om 10 uur gewekt door mijn moeder, die zegt dat er twee heren voor de deur staan die met mij willen praten over PC's. Ze hebben visitekaartjes met een of andere bedrijfsnaam er op.

Ik strompel naar beneden, vastbesloten om deze heren eens even vriendelijk te vertellen wat ik vind van mensen die om 10 uur 's morgens PC's komen verkopen. Door het luikje in de deur zijn inderdaad twee mannen zichtbaar, maar in plaats van mooie folders krijg ik een huiszoekings- en een arrestatiebevel onder mijn neus gedrukt.

De deur zit in het nachtslot, en dus kunnen ze niet naar binnen. Deze meneer ziet er echter nogal vastbesloten uit, en onze deur is van glas. Na razendsnel overleg in mijn plotseling bijzonder wakkere hoofd besluit ik dat het misschien het verstandigst is om gewoon open te doen.

Waar ze allemaal vandaan komen weet ik niet, maar ineens staan er twaalf man in mijn huis. Onder hen een rechter-commisaris, een officier van justitie (of een hulp-officier, weet ik veel) en een heleboel agenten. Nou lees je hierover wel eens in boeken en zie je het op de TV, maar je denkt toch niet zo snel dat het je zelf zal overkomen.

Ik ben nog enigszins beduusd als men mij vertelt dat ik mijn kleren aan moet gaan trekken. Nog geen 10 minuten later zit ik in een politieauto op weg naar Amsterdam (gillende sirene over de vluchtstrook). Bij mij thuis is (naar ik later hoorde) de rest van de politiemacht nog een tijdje bezig geweest om het hele huis overhoop te halen en al mijn computerspullen mee te nemen. Zelfs de Hack-Tics zijn weg.

De cellen van het hoofdbureau van politie in Amsterdam zijn niet bijzonder oncomfortabel. Er is een bed, een stoel en een tafel. Er is een luidsprekertje waaruit je SKY-radio kunt laten komen.

SKY is de enige zender waarop geen nieuws te horen is, ze vertellen zelfs niet hoe laat het is.

Ontspannen, ontspannen. Lukt niet! Die middag komen Coersen en v/d Wouw, leden van het Pilotteam computercriminaliteit Amsterdam mij ophalen voor het verhoor. Coersen tikt, v/d Wouw ondervraagt. Het lap-topje heeft eerst nog een lege batterij, en na veel gedoe komt er een verlengsnoer. WordPerfect (Yuk!) wordt opgestart en het verhoor kan beginnen.

"Wil je wat drinken?", "Je weet waarschijnlijk wel waarvoor je hier zit", "Begrijp je de aanklacht?". Heel gemoedelijk allemaal. Mij wordt verteld dat ik beschuldigd wordt van het inbreken in meerdere computersystemen. "Je hoort later wel welke systemen precies". De precieze beschuldiging is oplichting en valsheid in geschrifte.

Het begint met hele simpele vragen. "Weet je wat UNIX is?". Ze laten wat log-files zien waarin te zien is hoe iemand een systeem aan het kraken is. Ik beantwoord alle algemene vragen over computer-security. Ik ben immers redakteur bij Hack-Tic, dus daar weet ik wel wat van. Het idee van dit eerste verhoor is dat ik in mijn onzekerheid lange verhalen afsteek en dat ik alleen met wat simpele vragen een "beetje op weg wordt geholpen". Ik ben niet echt in een praatstemming en na een uurtje zit ik dus weer in mijn cel.

Het tweede verhoor is die woensdagavond van 7 tot 11. "Herken je deze logfile?", "Herinner je je dit gesprek op 23 februari?". Tapverslagen en logfiles komen op tafel en stukjes worden voorgelezen. Ik kan me weer heel weel niet herrineren (een aantal vragen gaat over dingen die al een tijd geleden gebeurd zouden moeten zijn). Het blijkt dat mijn telefoonlijn 3 1/2 maand getapt is geweest.

Met allerlei opmerkingen over mijn privégesprekken proberen ze duidelijk te maken dat ze "toch alles al weten" en dat het alleen maar goed voor mij zou zijn om te bekennen. Als je niet meewerkt krijg je immers meer straf, dat is algemeen bekend. Ze vragen urenlang door. Pas om elf uur wordt ik naar de cel teruggebracht omdat anders het cellenblok gesloten zou zijn. "Anders moet je bij mij thuis slapen" grapt er nog eentje.

Ondanks alles best nog lekker geslapen die nacht. Donderdag komt eerst mijn advokaat op bezoek. Hij vertelt me welke rechten ik heb, en ik hoor van hem wat er bij mij thuis allemaal gebeurd is sinds mijn arrestatie.

Tot groot ongenoegen van de politie blijkt de Nederlandse pers zich op deze zaak te hebben gestort. Kranten en omroepen hangen al bij de politie aan de lijn nog voordat ik goed en wel van Utrecht naar Amsterdam vervoerd was. Mijn verhoor van de vorige avond was dus een poging om snel een bekentenis los te krijgen. Men was immers gedwongen om nu snel met een persbericht over deze zaak te komen. In het geval van Rob en Harry (zie de vorige Hack-Tic) had men dagenlang de tijd om rustig zo'n persbericht op te stellen.

Nadat de advokaat weer is vertrokken volgt een derde verhoor. Eerst moet ik de verklaring van de vorige avond tekenen. Het blijkt echter dat ze mijn woorden wel erg vrij hebben opgevat. Tot grote woede van de twee politiemannen weiger ik te tekenen.

Het verhoor gaat door. Ze beweren dat er vanaf mijn telefoonlijn gehacked is in diverse computersystemen. Ik kan me daarvan niks herinneren. Ik geef dit antwoord op zo veel vragen dat ze er uiteindelijk maar een WordPerfect macro voor maken. Elke keer als ik "Daar kan ik me niets van herineren" zeg hoeft Coersen nu maar één toets in te drukken.

Ze willen erg graag het wachtwoord hebben voor de diskreet-drive op mijn systeem. Deze en andere vragen blijven zich herhalen in de daarop volgende verhoren. "Je maakt het alleen maar moeilijk voor jezelf", "we vinden het wachtwoord toch wel", "we weten alles toch al", alle verhoorcliches worden geprobeerd.

"Als je nu bekent kun je vrijdag nog naar het Europees kampioenschap PaintBall". Shit, daar weten ze dus ook al van. Handig, maar daar trap ik niet in.

De verhoren herhalen zich totdat die zaterdag Koomen, de leider van het Pilotteam zich er zelf mee gaat bemoeien. "Ik laat niet met me lummelen!" briest hij. Dit heeft niet zo veel effect, en dus laten ze me die zondag vroeg in de middag maar gaan.

Thuis alle kranteartikelen nog maar eens doorgelezen. Vanaf nu ga ik door het leven als de 'computercrimineel' en 'netwerkvernieler'. Ronald O. Belachelijk

Wachten

Dan begint het lange wachten. De inval is nu meer dan vijf maanden geleden en ik heb nog steeds mijn spullen niet terug. Ik weet ook niet wat er nu gaat gebeuren en wanneer. Eigenlijk is dat wachten nog veel vervelender dan in de bak zitten.

Moraal

Wat is nu de moraal van dit verhaal? Als je gearresteerd wordt heb je het recht geen vragen te beantwoorden tot je met je advokaat hebt gesproken. Gebruik dit recht! Die politiemensen hebben echt niet het beste met je voor, die willen je gewoon veroordeeld zien. Als je twijfelt is het vaak beter om je mond helemaal dicht te houden. Laat je niet intimideren, daar kicken ze alleen maar op.

RGB



Zit toch niet zo met die telefoon te klooien!

09-0 nummers

Het telefoonnet heeft drukke straten en pleinen, waar duizenden mensen hun gesprekken voeren. Er zijn ook hoekjes en gaatjes waar maar weinig mensen komen. Wie lang genoeg rondwandelt ontdekt zelf stille stukjes. Ontdek je plekje.

Het is me al een tijdje geleden opgevallen dat er nummers zijn die met 09-0 beginnen, terwijl er toch geen landnummers zijn die met een nul beginnen. Ik heb ze een beetje afgescanned. Hier is het resultaat:

09-01

Via 09-01 kun je telefoneren via het ISDN netwerk. Kennelijk is deze code bedoeld om de internationale centrale te 'dwingen' een digitale lijn te gebruiken. De kosten zijn (helaas) precies gelijk aan de kosten als je het gesprek gewoon via 09 maakt. Alleen de volgende landen zijn aangesloten:

1	Verenigde Staten	45	Denemarken
31	Nederland	46	Zweden
32	Belgie	47	Noorwegen
33	Frankrijk	49	Duitsland
358	Finland	61	Australie
41	Zwitserland	65	Singapore
44	Engeland	81	Japan

Bovendien zijn in deze landen lang niet alle steden aangesloten. In Nederland zijn b.v. alleen Rotterdam, Den Haag, Utrecht en Amsterdam aangesloten. Dit zijn de enige plaatsen die nu ISDN hebben.

Toevallig gevonden dingen tijdens het scannen: 09-013199200 reageert een beetje vreemd, een raar soort echo.

09-03

Is hetzelfde als 09, ik kan in ieder geval geen verschil ontdekken, zelfs de teller loopt even snel. Waarom? Goeie vraag.

09-05 en 09-09

Hier wordt het interessant. De PTT wil iets voor ons verborgen houden. Men is stiekum aan het testen met een dienst die ze 'Virtual Private Network' noemen. Volgens de PTT gaat het om een dienst waarmee bedrijven 'kwantum korting' kunnen krijgen op internationale gesprekken naar vast ingestelde nummers. Deze nummers worden via de bedrijfscentrale gekozen. Eén van de test-bandjes zegt 'Verificatie van uw telefoonnummer is niet mogelijk'. Dit duidt er misschien op dat men toegang verleent op basis van het opbellende telefoonnummer.

```
09 054 100        : 204
09 054 n000000    : 204, n=2-4
09 055 000        : 202
09 055 020        : 207
09 055 400        : 207
09 055 666        : 207
09 055 555        : 201
09 055 120        : in-gesprek
09 055 998        : 207
09 055 999        : 207
09 056 789        : vreemde tonen
09 056 xxx        : bestaat niet
09 091 0000000000: 204
09 092 0000000    : 204
09 092 11         : bestaat niet
09 092 10         : bestaat niet
09 092 90         : bestaat niet
09 093 00000      : 204
09 098 111000000 : 204
09 098 20000      : 204
09 098 400000000 : 204
09 098 521100000 : 204
09 098 521300000 : 204
09 098 53000      : 204
09 098 60000      : 204
09 098 71000      : 204
09 098 72000      : 204
09 098 80000      : 204
09 099 xxxxxxxxxx: ????
```

201 bedankt voor uw testoproep naar de feature switch, 2-0-1
this is the test number for world-wide vpn service, you have reached the vpn switch in the netherlands, 2-0-1

202 verificatie van uw telefoonnummer is niet mogelijk 2-0-2
your telephone number cannot be identified 2-0-2

204 virtual private network calls zijn niet toegestaan vanaf uw telefoonnummer 2-0-4
virtual private network calls are not permitted from your telephone number, 2-0-4

207 u heeft te lang gewacht, probeert u het nog eens 2-0-7
you have waited too long, please try again 2-0-7

208 incorrecte authorisatie code of bestemmingsnummer controleer het nummer en probeer opnieuw 2-0-8
incorrect authorisation code or destination number please check the number and try again 2-0-8

09-99-1111 en 09-99-777

Moet je zelf maar uitproberen, maar alleen als je het theewater op de kostenteller warm wilt stoken. ;-)

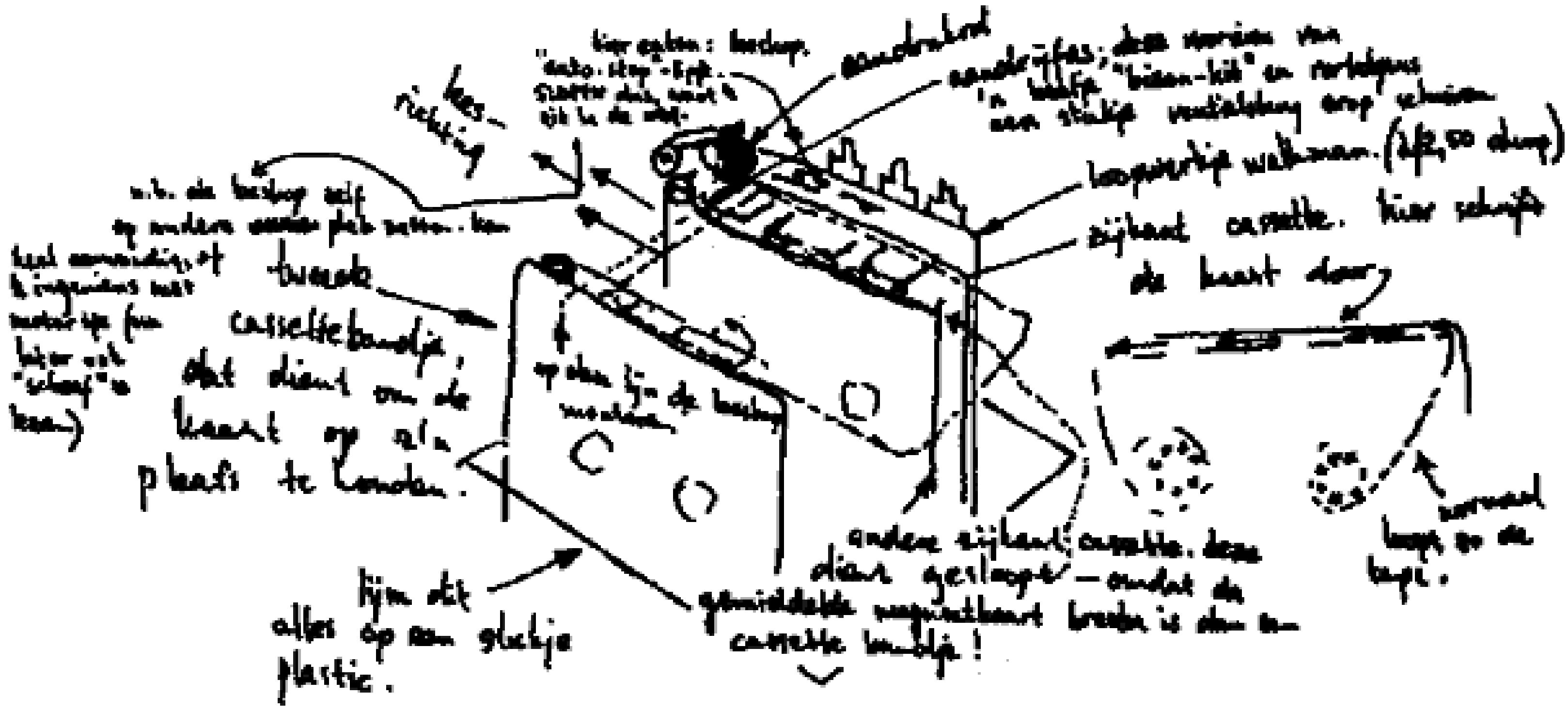
itsme

Waarde Hackers,

Naar aanleiding van een drietal Tic's die ik onlangs in bezit kreeg ("via-via"), enige opmerkingen. Tic 8 meldt ons trouwe lezertjes: "(...) alleen het mechanisme van een oude magneetkaart-lezer-schrijver komt hiervoor in aanmerking, tenzij je werkelijk een genie bent met draaibanken (...)". Het betreft hier het magneetkaartjesproject.

Met een walkmanloopwerkje en twee casettebandjes is echter een heel aardige benadering te maken. Niet voor mensen met twee linkerhanden natuurlijk, maar de inventief ingestelde hobbyist moet een heel eind kunnen komen.

Waneer je bovendien de motor op de walkmanelectronica aangesloten laat, beweegt de kaart (in theorie) met een keurige 4,75 cm/s langs de kop



Voorts: weet iemand hoe de PTT-telefoonkaarten werken? Als je ze schuin houdt bij een gloeilamp zie je iets glinsteren. Hoe langer dit "spoor", des te meer tikken op je kaart. Elke verbruikte tik wordt weggebrand. Maar: wat is dat glinsteren? Het is een soort holografisch gebeuren - "je ziet de regenboog". Nu dus nog de pot met goud.

V.

Onze electronici vinden het heel knap, maar beweren dat het je hiermee niet lukt om plastic magneetkaartjes te kopiëren, omdat het magnetisch materiaal daarvan veel te 'hard' is. Dat wil zeggen dat er grotere magneetvelden voor nodig zijn dan je met een casettekop kunt opwekken. Met kartonnen kopieerpasjes, parijse metrokaarten en italiaanse telefoonkaarten zou je met deze opstelling wel succes kunnen behalen.

Onder het stripje 'thermisch papier' op een telefoonkaart dat (soms) aangeeft hoeveel tikken je nog hebt, zit een stripje 'optische tralie'. Als je met een doek en spiritus geduldig wrijft komt deze strip vanzelf tevoorschijn. Deze tralie breekt in de telefooncel een bundel infrarood laserlicht. De tralie ligt onder een hoek van 45° ten opzichte van de richting van het stripje. Probeer zelf maar eens te experimenteren met een rode laser en je zult het wel zien. Deze tralie wordt inderdaad weggebrand. De cel checkt ook of ie echt weg is, dus afschermen werkt niet, tenzij je daarvoor materiaal gebruikt dat zelf ondoorzichtig wordt maar de kaart beschermt. Dit materiaal moet je dus elke keer vervangen. Wij horen mooie verhalen over blanke nagellak, bandensolutie en Tipp-Ex, maar we behalen zelf uiterst wisselvallige resultaten met deze spullen.

Een andere lezer stuurde ons ook gedetailleerde informatie over dit stripje, alleen heeft hij het over een hoek van 10 graden voor de nederlandse kaarten, terwijl wij zelf ongeveer 45° zien. We gaan in een volgende Hack-Tic zeker meer aandacht aan telefoonkaarten van alle soorten besteden. Lezers met interessante informatie: fax 020-6900968.

Aan: Hack-Tic

Er zijn 3 mogelijkheden:
1) Jullie zijn van de bvd, 2) Iemand bij jullie is van de bvd of 3) Jullie lijnen worden getapt
Dit was mijn laatste fax.
(Dit is serieus bedoeld, en als het optie 1 is zal dit wel niet in de Hack-Tic geregistreerd worden)

Geloof het of niet: dit is niet eens de idiootste brief die we kregen. Of deze nu naar aanleiding is van het artikel in Penthouse (zie pag. 3) geschreven is weten we niet, maar laat dit nummer nou net een soort paranoia-special zijn. Als we echt van de bvd waren hadden we dit niet geplaatst, tenzij we nou net willen dat jij denkt dat wij ....

Hello there

Fijn dat jullie mijn vorige brief over de veiligheidsgaten in Novell op waarde hebben weten te schatten en met zoveel inzicht hebben gebracht. Het patchen van ATTACH was nog niet bij me opgekomen, een erg inventieve oplossing, en een schouderklopje voor Itsme. Hierbij een nieuwe inlog-truuk. Deze berust niet op een bug in het Operating System, maar op een onnauwkeurigheidje van de betreffende supervisor. Toepasbaar op alle Novell-versies van 2.stenen.tijdperk tot en met v3.11.

Je kunt voor iedere gebruiker op het net die geen eigen login-script heeft zelf een script aanmaken. Je hebt namelijk create-rechten in de mail-directory van alle andere gebruikers, noodzakelijk om ze mail te kunnen sturen. Als er nog geen file staat die 'login' heet kun je die zelf aanmaken, compleet met een paar regels die jou security equivalent maken aan die gebruiker.

Let er wel op dat je de file niet meer kunt veranderen als je hem eenmaal hebt neergezet en dat de supervisor met NDIR altijd kan zien van welke login de file afkomstig is.

Johan de Wit

Geachte Hack-Tic

Naar aanleiding van het gratis bellen in Hack-Tic nummer 13 heb ik een aantal vragen. Ik veronderstel dat het tabelletje "Home Country Directs" ook landen bevat die nog een C5 centrale gebruiken. Ik dacht dat Brazilië nog wel redelijk achter lag, dus heb ik me geconcentreerd op dat nummer (06-0220655). Als ik dat bel krijg ik inderdaad een pliek te horen als ze oppakken. Is dat de juiste pliek?

Zo ja, dan zou ik tonen moeten kunnen meesturen. Ook over die tonen heb ik nog enkele vragen. De "MF-tonen" tabel geeft een lijstje met de bewuste tonen. Maar wat moet ik me voorstellen bij bijvoorbeeld een Clear Forward? Zijn dat twee tonen, eerst 2400 Hz gedurende 50 ms, gevolgd door 2600 Hz 50 ms, of is het één toon, bestaande uit de mix van die twee frequenties?

Overal waar een plusje staat in de tabel in hack-Tic 13 bedoelen we dat de twee tonen tegelijkertijd klinken. Het is dus inderdaad een mix van die twee tonen. Dat van Brazilië is inderdaad de juiste pliek, maar als je een CF geeft wordt de lijn opgehangen. Men maakt gebruik van een 'timed release'. Met andere woorden: als er een CF wordt ontvangen dan zendt Brazilië een 'Clear Back' uit met een minimale lengte, lang genoeg om jou van de lijn te gooien.

Er zijn nog wel landen waarmee het lukt, maar de spoeling begint wat dun te worden. Phreaking wordt echt iets voor de mensen met veel uithoudingsvermogen.

Waarde Hack-Tic,

Een van mijn medestudenten heeft stage gelopen bij de CRI en kon kleurrijk vertellen over hoe de Hack-Tic daar wordt gelezen. Er wordt echter een lijst bijgehouden van personen die bij de Hack-Tic betrokken zijn enzo. Omdat ik nog in dienst moet en dit soort grappen het verschil kan uitmaken tussen 16 maanden bij het Defensie Computer Centrum of 14 maanden wachthuisjes schilderen maak ik de 40 gulden voor de zekerheid over vanaf een rekening met de obscure naam <XXX>.

Interessant. Als je zo graag bij het Defensie Computer Centrum wilt, hebben wij nog wel een interessante collectie virussen voor je liggen. Ik denk dat ze niet kunnen wachten tot ze je binnen hun veilige muren hebben! Wel jammer dat die lieden een democratie moeten verdedigen waarin het nou net zo belangrijk is dat je zelf mag weten wat je leest.

Geachte Tic,

Virussen worden de laatste drie jaar steeds vaker commercieel geëxploiteerd. Een paar maal heeft Nederland al op z'n kop gestaan toen er bekend gemaakt werd dat op een bepaalde datum een allesvernietigend virus aktief zou worden. Als je dan achteraf hoort dat slechts een paar wat grotere bedrijven schade hebben geleden (namen van de bedrijven hoor je al helemaal nooit) dan begint er toch iets te stinken waarvan men altijd zegt dat het dat niet doet.

Van een van de bedrijven die aan deze 'race tegen het virus' meedoet heb ik onlangs de 'virus-kalender' mogen ontvangen. Hierin word ik alvast gewaarschuwd voor de vele uiterst gevaarlijke virussen die in aantocht zijn, bijna als of ze ze zelf schrijven. Natuurlijk heeft dit bedrijf ook een (bepaald niet kostenloze) oplossing voor deze plaag. Ook als ik al getroffen ben door een virus kunnen ze dat voor me verwijderen.

Check de kalender voor je een besmetting meldt! Doe je het op een datum waarop geen virus aktief wordt dan schrijven ze er misschien wel eentje speciaal voor jou. Wat is gevaarlijker, virus of dokter?

Cyberpunk 3

Geachte PTT Telecom,

Ik heb ontdekt dat je ook als brave burger 'gratis' kan bellen; Laatst belde ik vanuit een blauwe telefooncel in Boedapest naar Nederland. Na inworp van in totaal 85 Ft. was de telefoon vol. Aan het einde van het telefoongesprek kreeg ik 65 Ft. weer terug, dus de totale kosten bedroegen 20 Ft, omgerekend zo'n 50 cent. Of het bij elke cel werkt weet ik niet, maar hij deze heb ik het meerdere malen geprobeerd. Het is de meest rechtse bij de metro-ingang op Felszabadulas ter / Ferenciek. Let op: gele cellen=alleen nationaal bellen en oud; rood=ook internationaal bellen, oud; grijs=alleen nationaal, oud roest en blauw=internationaal en nieuw, of alleen alarmnummers.

Nog een voorval: Op mijn school staat een mooie oude telefoon met kwartjesvenster. Gratis bellen dacht ik. Fout! Als je zonder inworp van kwartjes een nummer draait (met een TDK-doosje) wordt de hoorn afgesloten indien er opgenomen wordt. Dus kan ik niet met mijn vriendinnetje in het buitenland bellen. Uit verveling gooi ik een kwartje in het toestel, bel een nummer met het TDK-doosje, realiseer me dat dit niet het goede nummer is, geef een korte tik op de haak (zodat het geld blijft staan), krijg de kiestoon en bel vervolgens toch naar mijn vriendin. Na een uurtje bellen zonder de hinderlijke pieptoon gooi ik de hoorn op de haak en krijg mijn kwartje terug. De telefoon weigert ook daarna alle geld, maar bellen kan nog wel. Het kwartje is klem blijven zitten en de telefoon denkt dat hij 'vol' zit. Meer research is nodig, maar gezien mijn reputatie op school kan iemand anders dat beter doen.

Ik hoop dat jullie kunnen voorkomen dat hier misbruik van gemaakt wordt, want het lijkt me sneu als de betreffende instantie een hoge rekening en een leeg geldbakje vindt.

Brave Burger

De polariteit is verkeerd om aangesloten, normaal blokkeert de cel de microfoon voordat er opgenomen wordt aan de andere kant, en niet erna. Als je ons even het adres van je school geeft zullen wij ze wel waarschuwen.

Afluisteren met de hoorn op de haak

Je hebt het deze zomer in de kranten kunnen lezen en op TV kunnen zien: het is mogelijk om het geluid in een ruimte af te luisteren door de microfoon van een telefoontoestel waarvan de hoorn op de haak ligt.

Hoe hard de PTT ook beweerde dat het onzin was: een simpele demonstratie deed wonderen. De camera's van KRO Brandpunt registreerden hoe het door ons gebouwde apparaat vanuit de slaapkamer keurig het geluid in onze woonkamer liet horen. In dit artikel niets over de politieke achtergronden en geen woord over de rechtszaak waarin dit alles een rol speelde. Hier is slechts de rauwe techniek waar het allemaal om draait.

Hoogfrequente wisselstromen

Als je een T-65 telefoon van de PTT zou openschroeven en je zou de printbanen volgen, dan zou je opvallen dat het haakcontact de microfoon afsluit op het moment dat de hoorn op de haak wordt gelegd. Het is dus niet mogelijk om de microfoon te gebruiken zolang de hoorn op de haak ligt, er kan immers geen stroom doorheen lopen. Voor gelijkspanning is dat waar, maar voor een hoogfrequente wisselspanning werkt het haakkontakt als condensator. Een condensator is immers in essentie niets anders dan twee dicht bij elkaar gemonteerde plaatjes.

De centrale zet een gelijkspanning op de lijn, en als de hoorn wordt opgepakt zal er een stroom door de telefoon gaan lopen. Deze stroom wordt gemoduleerd met het spraaksignaal. Door in plaats van deze gelijkspanning een wisselspanning op de lijn te zetten kunnen we stroom door het toestel laten lopen zonder dat de hoorn opgetild hoeft te worden. Deze wisselstroom wordt dan, net als de gelijkstroom wanneer de hoorn is opgetild, gemoduleerd door de microfoon in de hoorn.

Op de volgende pagina's een bouwsel dat de basisprincipes demonstreert. Verwacht hiervan geen hi-fi.

Bij het schema

De 4046 wordt gebruikt als goedkope VCO (Voltage Controlled Oscillator). Met de 33k weerstand op pin 11 werkt hij tussen de 30 tot 350 kHz. Met de potentiometer kun je de frequentie instellen. De uitgang van de 4046 kan niet genoeg stroom leveren om de spoel te laten resoneren. De transistors versterken de stroom zo'n honderd maal.

De spoel is instelbaar tussen de 1 en 50 miliHenry. Deze spoel vormt samen met de capaciteit van de telefoon een afstemkring. We brengen de telefoon in resonantie om een voltage op de lijn te krijgen dat hoog genoeg is om de microfoon te activeren. Alleen op het punt waarop de telefoon resoneert verdwijnt alle ruis en wordt het

geluid in de kamer hoorbaar. De spoel wind je liefst om een kern waarbij al gegevens zitten die je vertellen hoeveel windingen je nodig hebt om tot de gegeven inducties te komen.

Tussen de spoel en de telefoon zit een diode die het signaal oppikt. Het simpele detectorschakelingetje scheidt de audio van het hoogfrequente signaal. De audio wordt tenslotte gefilterd en naar buiten gebracht, alwaar het verder wordt versterkt en hoorbaar wordt gemaakt. Het audio filter is maar een suggestie, zeker voor verbetering vatbaar. Echte freaks kunnen zelfs DSP techniek gebruiken om het signaal beter uit de ruis tevoorschijn te toveren. Als er een erg lange draad zit tussen de afluisteraar en het toestel zul je dit soort technieken wel nodig hebben, het signaal wordt dan *erg* zwak.

Om optimale resultaten te behalen moet je het ingangsvoltage van de schakeling tussen de 5 en 18 volt kunnen varieren om het maximale geluidsniveau te krijgen. Hiervoor dient potmeter P2 in de voedingsschakeling onderaan de tekening.

Als je iemand op deze manier afluistert kan hij of zij de telefoon niet gebruiken. In plaats van de telefooncentrale is hij/zij immers met jouw electronica verbonden. De LED D3 geeft aan wanneer de aangesloten telefoon wordt opgenomen. In plaats van de LED kun je natuurlijk ook een schakeling zetten dat razendsnel de PTT-lijn met het toestel verbindt.

De bediening van dit geheel is in theorie erg simpel: Zet om te beginnen de spoel op 10 mH en ga eens aan de frequentie draaien. Zoek naar 'stille plekken'. Probeer tijdens het testen verschillende T-65's. In sommige telefoons liggen de kontaken in de 'op-de-haak-stand' dichter bij elkaar dan bij andere. Dit verklaart dat sommige telefoons met deze methode veel beter af te luisteren zijn dan andere.

Doe jezelf een lol, bouw deze schakeling niet tenzij je al eerder hoogfrequente electronica hebt gebouwd. Dit is niet bedoeld als eerste zelfbouwproject. Als je niet in staat bent om dit soort schakelingen te 'debuggen' kun je dit project wel vergeten.

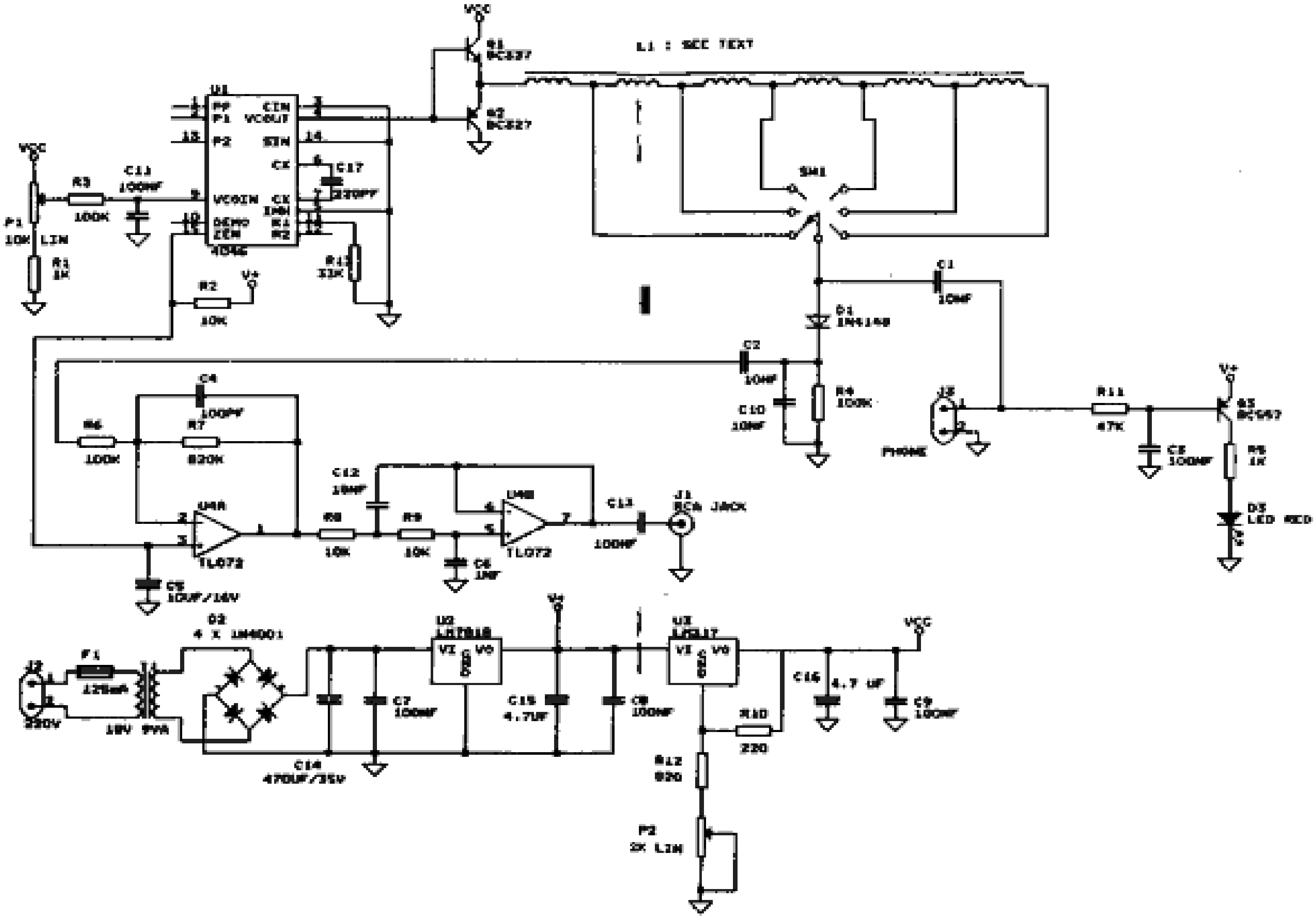
Tegenmaatregelen

Nadat de PTT moest toegeven dat bepaalde telefoons op deze manier kunnen worden afgeluisterd kwamen ze al snel met het tegenmiddel op de proppen. Als je een condensator van 33 nanofarad parallel met de telefoon zet loopt alle hoogfrequente stroom door deze condensator, en blijft er dus niets over voor de telefoon. Deze condensator van 20 cent was bij de PTT te koop voor 6 en een halve gulden. Ingebouwd in een luxe telefoonstekker, dat wel. Ik zeg *was* te koop, want ik heb hem al maanden niet meer gezien in de Primafoonwinkels.

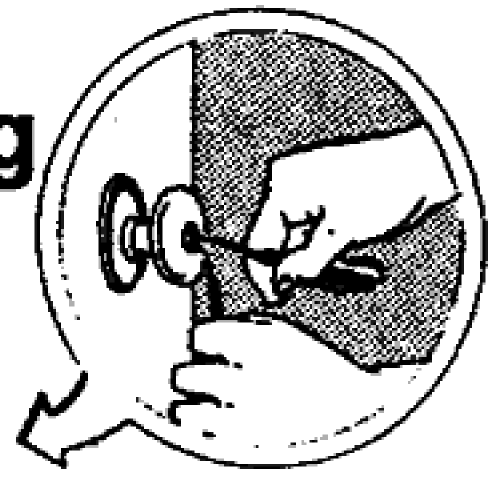
Eerste experimenten lijken uit te wijzen dat die condensator inderdaad afdoende werkt tegen deze afluistermethode, maar het is theoretisch mogelijk dat je bij bepaalde telefoons ondanks de condensator toch nog genoeg stroom kunt laten lopen om een hoorbaar signaal te produren.

Billsf

Afluisteren met de hoorn op de haak



Lock Picking



Deel 1 Door The Key

Dit artikel gaat over het openmaken van sloten waarvoor je geen sleutel hebt, zonder het slot te beschadigen. Bij gebrek aan een goede Nederlandse naam voor deze behendigheid zal ik de Engelse benaming 'Lock Picking' gebruiken.

Het kan zijn dat je dit artikel leest omdat je de hierin beschreven vaardigheden wilt gebruiken voor inbraak, diefstal en wat dies meer zij. Hier is goede raad: koop een boor, een paar schroevedraaiers, een hamer en een breekijzer. Echte meesterlockpickers kunnen een slot soms weliswaar net zo snel openmaken als mensen met primitieve gereedschappen, maar deze meesters van het vak doen dan ook al jaaaaren niets anders.

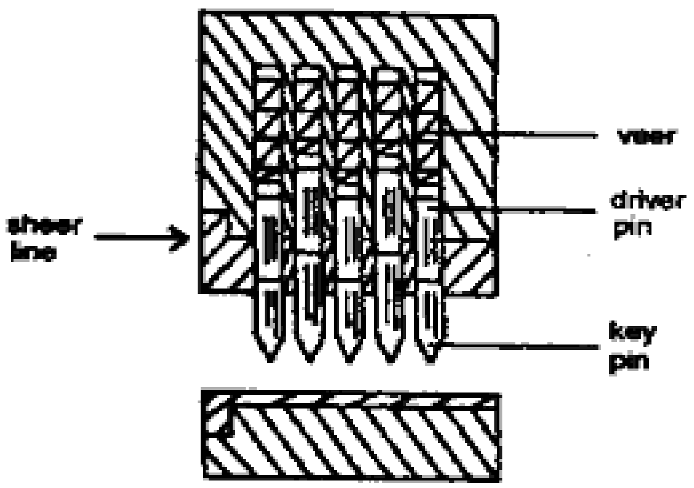
Lockpicking is een vaardigheid die je bij uitstek gebruikt om ongemerkt rond te sluipen op plaatsen waar je niet mag komen. Zo maken geheime diensten regelmatig van deze vaardigheden gebruik. Deze serie artikelen geeft geen oordeel over het gebruik van deze technieken, maar beschrijft alleen in zo veel mogelijk detail hoe sloten moeten worden opengemaakt zonder ze stuk te maken. Verder zul je lezen hoe je je eigen gereedschap kunt maken en wat voor moeilijkheden de makers van sommige sloten hebben ingebouwd.

Een schriftelijke cursus lockpicking is misschien net zo zinvol als een schriftelijke cursus sex. Je moet het vaak doen om er goed in te worden. We kunnen je hooguit wat tips geven die je kunnen helpen bij het oefenen.

Sloten en sleutels

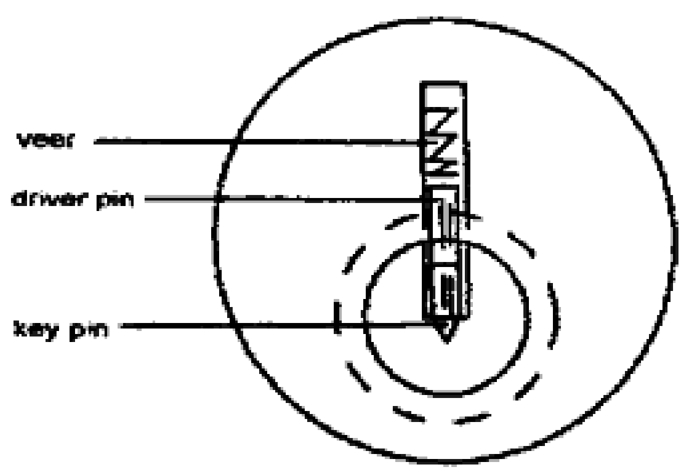
Deze serie gaat hoofdzakelijk over cylindersloten. Ouderwetse baardsloten worden zo zeldzaam dat het ook weinig zin heeft om daar veel aandacht aan te besteden.

Voordat er ook maar iets in een slot gestoken wordt moeten we eerst weten hoe een slot werkt. Een doorsnede van een cylinderslot zie je hierboven.

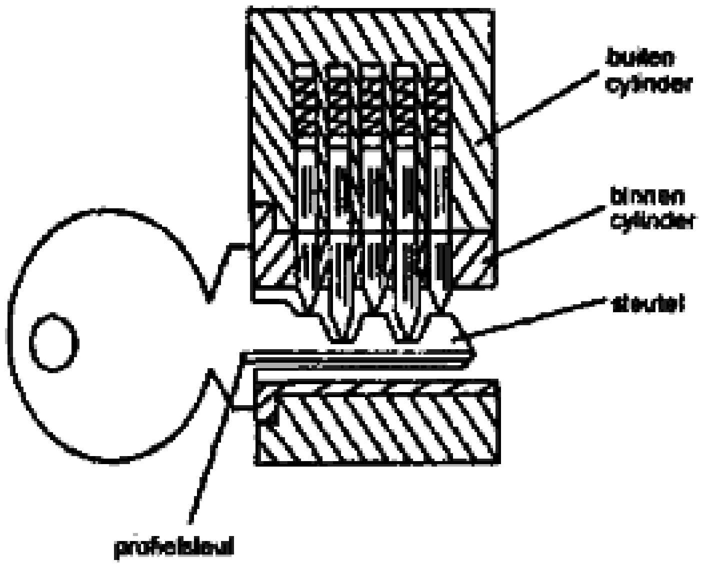


Doorsnede cylinderslot in rust

In ruststand worden alle pins door de veren achter de driver pins helemaal naar beneden geduwd. De driver pins zakken gedeeltelijk in het slot en blokkeren de draaing van het slot. Van voren ziet dat er dus als volgt uit:



Een in het slot gestoken sleutel drukt tegen de key pins. Deze drukken de driver pins omhoog in de daarvoor geboorde gaten in de buitencylinder van het slot. De key pins zijn van verschillende lengte, en alleen als de breuklijn tussen key pins en driver pins overal gelijk ligt met de overgang tussen binnen- en buitencylinder kan het slot draaien.



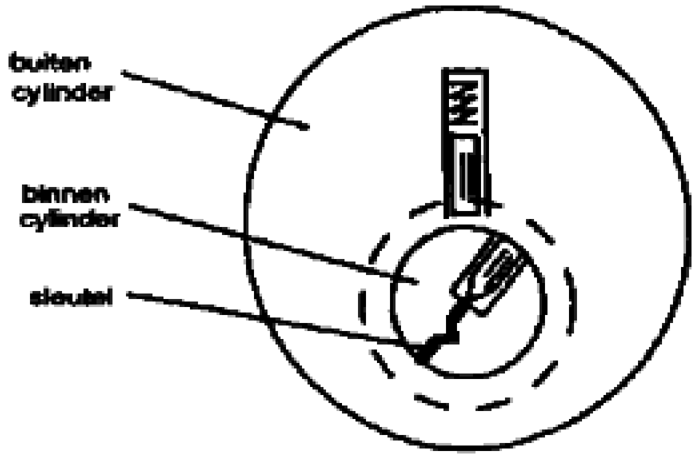
Doorsnede slot met sleutel

Deze lijn noemen we (in goed Engels) de 'sheer line'. Als de binnencylinder draait kun je het slot openen. De buitencylinder wordt in Engelse literatuur 'hull' of 'shell' genoemd, de binnencylinder 'plug'.

Niet elke sleutel past in elk slot. Elk type cylinder heeft een eigen 'profiel'. Sleutels met een verkeerd profiel passen niet eens in het slot. Sleutels met het juiste profiel, maar de verkeerde inkepingen ('cuts') passen wel in het slot, maar het slot wil niet draaien. Sommige key-pins zijn gedeeltelijk doorgedrukt tot in de buitencylinder (de cut in de sleutel is niet diep genoeg), sommige driver pins zitten gedeeltelijk nog in de binnencylinder (cut is te diep).

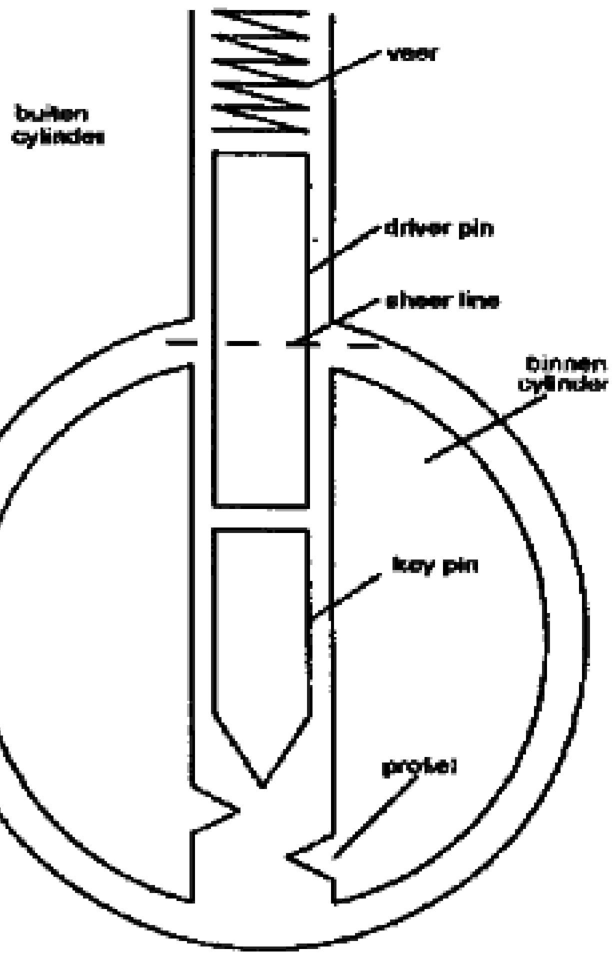
Als je het bovenstaande niet helemaal begrijpt, kijk het dan nog maar eens rustig door, want als je dit niet snapt is er geen enkele kans dat je OOIT succesvol een slot kunt picken.

Hoeveel pins een slot heeft hangt af van



Vooraanzicht slot met sleutel

het type slot. De meeste huis- en kantoorsloten hebben 5 pins, een hangslot heeft meestal 4 tot 6 pins. Speciale veiligheidssloten hebben soms wel zeven of meer pins. Het mag duidelijk zijn: hoe meer pins, hoe moeilijker het is om het slot open te krijgen, het is immers meer werk om alle pennen tegelijkertijd op de juiste plaats te krijgen.



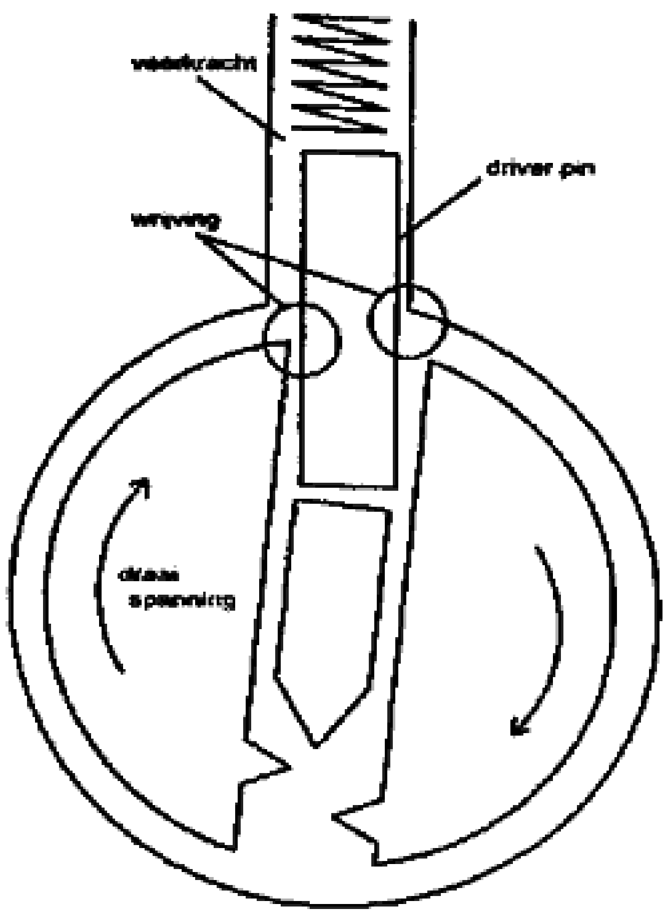
Slot in rust

Hoe werkt Lockpicking?

Als een slot precies volgens de bovenstaande theorie zou werken dan zou het niet te picken zijn. Er zou immers geen manier zijn om uit te vinden in welke stand alle pins moeten staan. Alle combinaties proberen gaat ook niet, daar zouden jaren overheen gaan.

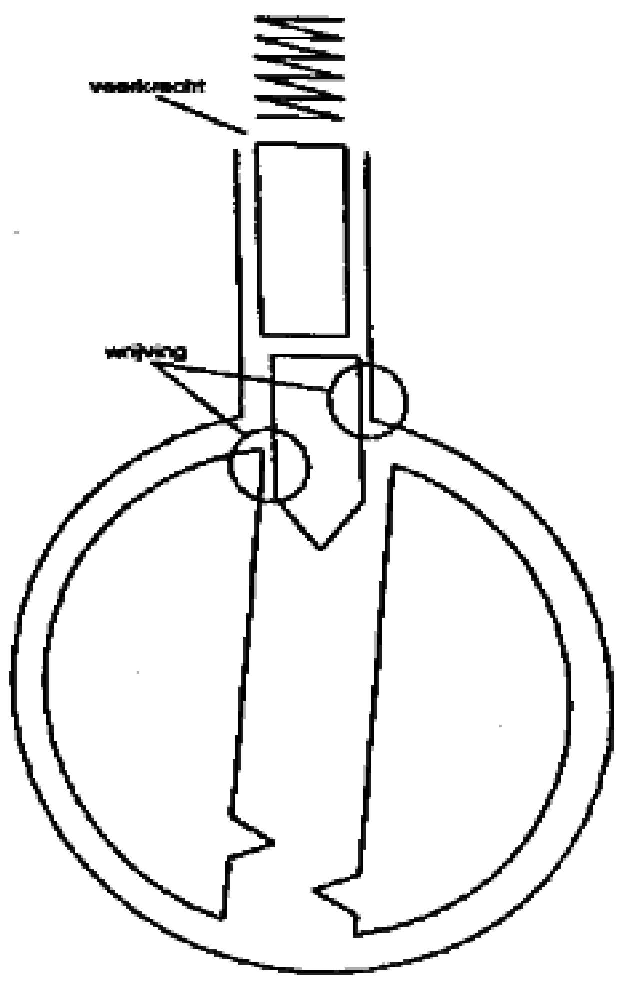
Geen enkel slot werkt precies zoals de theorie dat wil. In elk slot zit een speling tussen de pins en de gaten waarin ze heen en weer bewegen. Ook zitten deze gaten nooit helemaal op één lijn, en zit er altijd een speling tussen binnen- en buitencylinder.

Als op een slot een lichte draaikracht wordt uitgeoefend, dan komen de driver pins klem te zitten tussen de binnen- en de buitencylinder. De bovenstaande factoren zorgen ervoor dat bepaalde pins meer klemmen dan anderen.



Slot onder spanning

Om te kunnen lockpicken is het van belang om precies zoveel spanning te zetten dat de pins wel klem zitten, maar dat je ze nog kunt bewegen. Het draaien van het slot doe je met een spanner, het bewegen van de pins met een lifter. De spanner kan gewoon een stukje gebogen veerstaal zijn, smal genoeg om aan de onderkant in het slot te passen, en breed genoeg om een klein beetje kracht te kunnen zetten. De spanner steek je dus onder in het slot, dus niet aan de kant waar de pinnen de binnencylinder binnen komen. Vervolgens draai je de spanner dezelfde kant op die je normaal met een sleutel zou draaien.



Te ver

Omdat er geen sleutel in het slot zit blokkeren de pins nu het slot. Hoe makkelijk een slot te spannen is, is afhankelijk van het profiel. Soms heb je erg weinig ruimte, dan heb je een smalle spanner nodig, en soms is het slot zo breed dat je spanner 'wegglijdt', dan heb je een bredere spanner nodig. Neem de tijd om het slot te spannen; zonder de

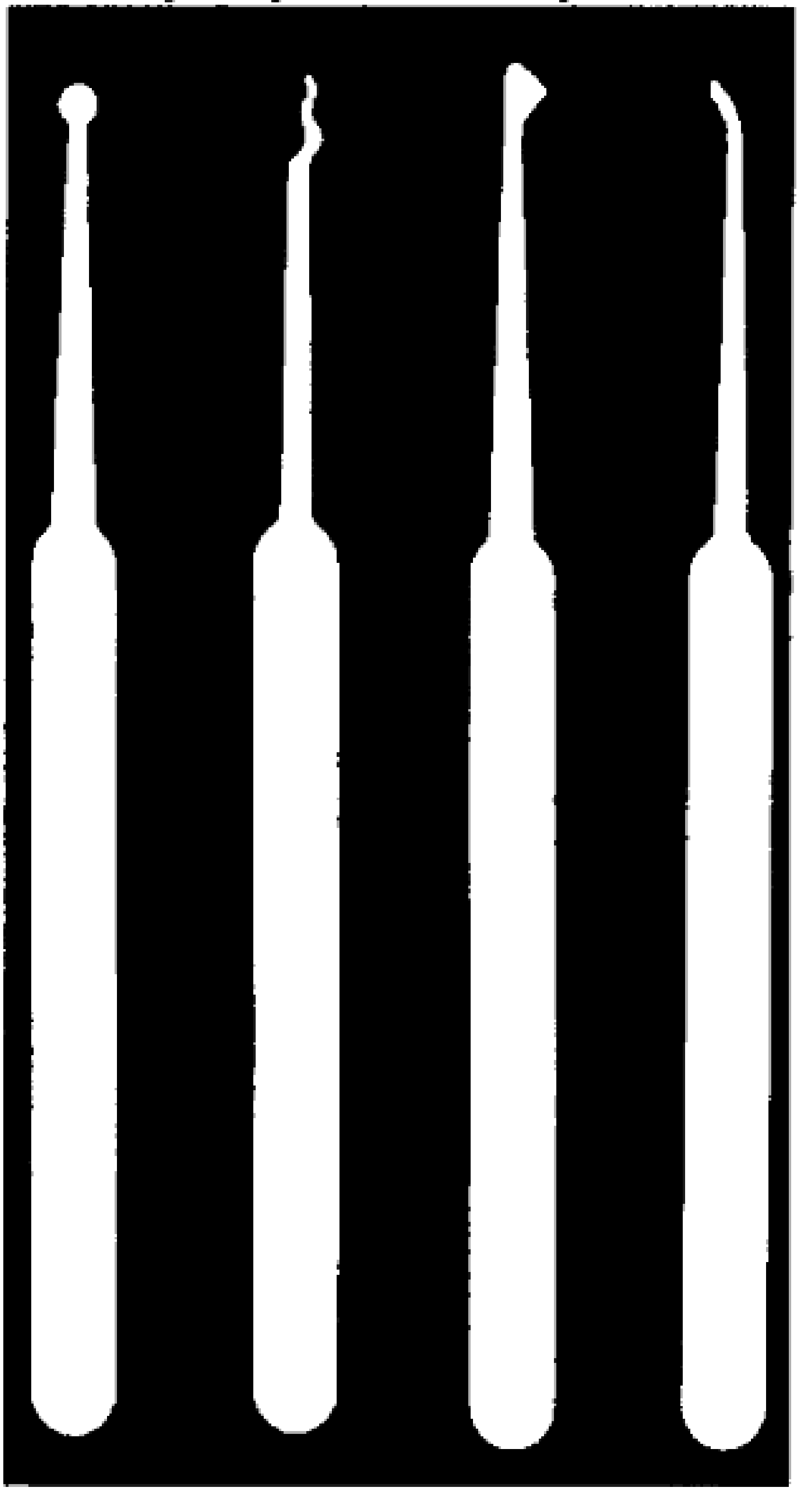
juiste spanning bereik je met de beste gereedschappen helemaal niets.

Als je de pins een voor een aanraakt voel je dat een van de pins het 'strakst' zit. Deze pin beweeg je omhoog totdat je voelt dat de binnencylinder een heel klein stukje verder draait. Als het goed is dan is de driver op de buitenkant van de binnencylinder blijven liggen, en ligt de key pin dus los in de binnencylinder.

Als de pin eenmaal op de binnencylinder ligt zal een andere pin het slot blokkeren. Vind deze pin en pas hetzelfde truukje toe, totdat alle pins uit de weg zijn en het slot is open. Ga je met een pin te ver en voel je dat het slot blijft blokkeren dan laat je de spanning wegvallen (alle pins worden teruggeduwd) en begin je opnieuw.

Tools

Je kunt lock-pick sets kopen. In Nederland zijn ze alleen te koop voor sleutelmakers (met papieren van de Kamer van Koophandel). Kopers van sommige meer specialistische stukken gereedschap worden door de leverancier geregistreerd. Betaal voor een basis-set lock-picks (6 - 10 lifters plus spanner) niet meer dan 75 à 100 gulden.



Ik heb nog wel eens een paar setjes liggen, als je interesse hebt kun je kontakt opnemen met box 101 op de Hack-Tic VoiceMailBox. Je kunt ook naar Hack-Tic schrijven of faxen, t.a.v. The Key.

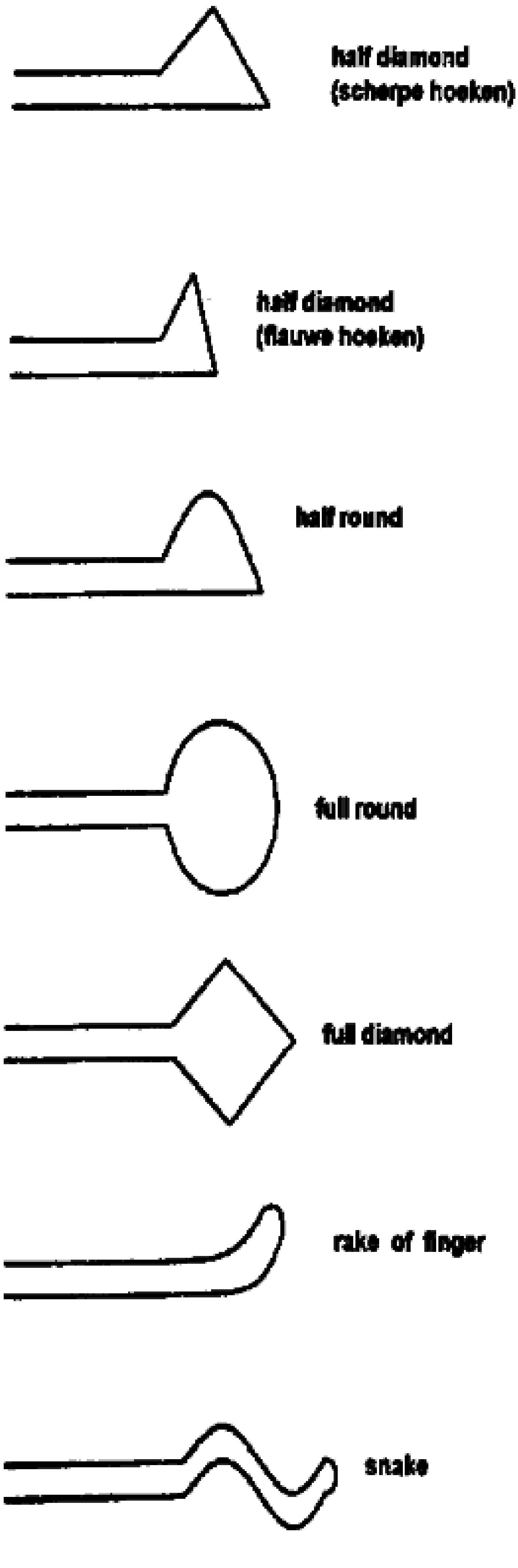
Je kunt je gereedschap ook zelf maken. Hier is een recept:

Benodigdheden: genoeg hardmetalen ijzerzaagjes en een slijptol. Als spanner gebruik je het afgebroken metalen clipje van een oude balpen. Als het goed is is dat een L-vormig stukje metaal. Zorg dat je er eentje hebt van een beetje buigzaam metaal, niet te dik, en niet te kort. Eventueel het kopje (dat in het slot moet) een beetje bijvijlen.

De finger-pick (ook wel 'rake' genoemd) is een van de belangrijkste lifters. Je zult merken dat je voor een heleboel sloten eigenlijk niet meer nodig hebt dan een spanner en deze lifter. Hiernaast is een kleine maar volledige lock-pick set op ware grootte afgebeeld.

Op de volgende pagina staat een meer volledige set met benamingen. In beide sets is de spanner niet afgebeeld.

Je maakt deze lifters door met een slijptol een ijzerzaagje te bewerken.



Doe steeds kleine beetjes tegelijk en koel het zaagje daarna af in een bakje water. Zet het water naast de slijptol zodat je niet te veel tijd verliest tussen slijpen en koelen. Nooit langer dan een paar seconden slijpen, en bij de dunne stukken niet langer dan één seconde. Een lifter die bij de fabricage oververhit is geraakt zal snel buigen of breken.

PAS OP: Zorg bij dit werkje voor handschoenen en een veiligheidsbril.

Waar je al deze lifters voor gebruikt is in de lock-pick-literatuur nogal onderhevig aan de smaak van de auteur van het artikel dat je aan het lezen bent. Men is het er over eens dat de full-round en full-diamond vaak nodig zijn om sloten open te krijgen die aan twee kanten pennen hebben (auto's).

De half-round is handig bij disc-tumbler sloten, oftewel 'schijfjes-sloten'. Deze vind je in veel kantoren op de bureauladen, en op brievenbussen. We behandelen deze sloten meer gedetailleerd in het volgende nummer. De snake-lifter komt goed van pas bij een andere methode van lock-picken: scrubbing. Ook hierover meer in het volgende nummer.

Oefenen: niet op straat.

Koop om te beginnen een paar goedkope sloten. Haal bij vrienden en kennisen alle ongebruikte hangsloten en oude cylindersloten weg. Op de markt hebben ze vaak goedkope (en slechte) hangsloten. Om te oefenen is voorlopig het slechtste nog niet slecht genoeg: je moet makkelijk beginnen. Kijk je lokale sleutelboer eens lief aan en vraag of hij/zij nog oude sloten heeft liggen. Rondkijken in winkels met veel sleutels en sloten is sowieso NOOIT verspilde tijd. Veel sleutelfabrikanten leveren mooie kleurenplaatjes met opengewerkte sloten om te laten zien hoe veilig het allemaal is.

Pak een makkelijk hangslot (maximaal 4 pennen) en probeer de beschreven technieken uit. Let er op dat je niet te veel of te weinig spanning op het slot zet (uitproberen!). Gebruik de finger-pick om te voelen hoe strak het slot zit terwijl je de spanning varieert. Maak je niet druk als het

allemaal niet direct lukt. Lukt het je om een goedkoop slotje open te krijgen dan kun je wat moeilijkere sloten proberen. Elk slot is anders.

Als twee pennen ongeveer even strak zitten moet je altijd de achterste het eerst picken omdat de kans groot is dat je daar in een later stadium moeilijk bij kunt zonder andere pins te bewegen.

Bouw een beeld in je hoofd op van wat er in het slot gebeurt. Probeer je ogen niet te gebruiken: je ziet toch geen moer (behalve de eerste pin) en in echte situaties heb je je ogen vaak veel te hard nodig om op je omgeving te letten. Lockpicking en Zenboedisme hebben het nodige gemeen. Concentratie is het motto.

Het moet nog maar eens gezegd worden: alleen met veel oefenen kom je ergens. Niemand kan onmiddelijk elk voordeurslot open krijgen. Begin met simpele slotjes. De techniek van lockpicking kan worden geleerd volgens de 3 O's: Oefenen, Oefenen, Oefenen!

The real thing

Op je oefensloten was het leven nog redelijk gemakkelijk. Zodra een van je vrienden z'n sleutel weer eens heeft vergeten liggen er nog een paar extra problemen op de loer. Voor we beginnen: ligt er geen sleutel onder de mat/op de kast naast de deur/in de bloembak/onder de vuilnisbak/etc? Ten tweede: zit de deur wel op slot? Niets is frustrerender dan het picken van een open slot!

No luck? Aan de slag dan maar. De betere lock-picker weet van elk merk al een beetje wat hij kan verwachten. Als je genoeg geoefend hebt moet je nu ook onbekende sloten de baas kunnen: het duurt alleen langer.

Is er ruimte in het slot voor tensioner en pick? Sommige sloten hebben een profiel dat maar bar weinig ruimte laat. Lastig, maar nog steeds te doen. Rustig werken, anders beschadig je je gereedschap.

Welke kant zal het slot draaien? Het is lullig om 20 minuten te peuteren en dan uiteindelijk te merken dat je het slot op het nachtslot hebt gezet. Als het slot al op het nachtslot staat moet je het slot meerdere malen rond draaien. Hou er rekening mee dat alle pins dan dus terug vallen en je weer opnieuw moet beginnen. Je kunt proberen om het slot zeer snel te draaien, maar veel kans maak je niet.

Hoeveel pins heeft het slot, en hoe lastig voelt het? Je moet weten wanneer iets geen zin heeft. Een onervaren lock-picker kan een slot met zes of zeven pins wel vergeten, een slot met 5 pins is al een hele kluif!

Werk met je handen en je hoofd, gebruik je ogen om om je heen te kijken.

Veel succes bij het maken van je gereedschap en bij het oefenen.

In de volgende Hack-Tic staat deel 2 van deze serie. Daarin onder andere:

- Meer technieken
- "Moeilijke" sloten
- Ronde sloten, kruissloten
- Moedersleutels

Utrechtse PTT hielp spionnen van politie

Van een verslaggever

... twijfels over de affaire, die de Utrechtse advocaat mr. Bernhard Tomlow aan het licht brengt.

... post van de afgelopen ... zijn achtergehouden ... advocaat ... Utrechtse ...

Mr. Tomlow stelt dat ... medewerking aan ...

D'66 wil opheldering over afluisteren door inlichtingendiensten

Van onze verslaggever

DEN HAAG — De D'66-fractie in de Tweede Kamer wil dat de regering opheldering geeft over afluisterpraktijken van de Inlichtingen Dienst Buitenland (IDB) en de Marine Inlichtingen Dienst (Marid). Beide diensten houden zich bezig met het afluisteren van ambassades in Den Haag. D'66 wil zekerheid dat deze geheime activiteiten zich niet uitstrekken tot burgers.

Afluisteren van telefoongesprek ruim 1000 keer

DEN HAAG, 20 juni — In 1985 is in 1087 gevallen toestemming verleend voor het afluisteren en opnemen van telefoongesprekken ten behoeve van de strafvordering. Minister Korthals Altes van justitie meldt dat in een brief aan de Tweede Kamer.

Regels bij afluisteren telefoon soepeler

DEN HAAG – De wettelijke regels voor het afluisteren van telefoons door politie en justitie worden gewijzigd. De telefoontap wordt losgekoppeld van het zogeheten gerechtelijk vooronderzoek. Wel blijft toestemming van een rechter nodig.

Criminelen kunnen gemakkelijk afluisteren

Vakbondsleiders afgeluisterd

Afluisterpraktijken van politie lopen vooruit op wetgeving

Van onze verslaggever
JOS SLATS

AMSTERDAM — De politie-praktijk heeft de politieke praktijk ingehaald. Terwijl het wetsvoorstel dat de politie ruimere bevoegdheden geeft bij het afluisteren van telefoons nog moet worden behandeld door de Eerste Kamer, wordt hier en der in het ...

... „Ik denk dat de bestaande wet die interpretatieruimte wel biedt."

Minister Hirsch Ballin van Justitie denkt daar anders over, want hij maakt in een wetsvoorstel wel onderscheid tussen telefoongesprekken en communicatie via fax, telex of computer. De minister vindt dat de politie voortaan ook deze communicatiemiddelen mag ...

... bevestigen dat — blijkt uit tapverslagen dat de politie steeds vaker een vrij goed beeld heeft bij het afluisteren van criminelen. „Dan ben je opeens dat een verdachte per ongeluk ... op de hoorn heeft gelegd, waardoor de afgeluisterde telefoon ... gaan functioneren als een verborgen microfoon. Endoscopie — ...

Doorschakelen hindert justitie

Afluisteren telefoon bemoeilijkt

(Van een verslaggeefster)

AMSTERDAM – De nieuwe doorschakelservice van de PTT blijkt problemen op te leveren bij het aftappen van telefoongesprekken van criminelen door justitie. Technisch blijft het aftappen van een doorgeschakelde lijn weliswaar mogelijk, maar hiervoor moeten in sommige telefooncentrales speciale voorzieningen worden getroffen.

Politie plaatst taps op openbare telefooncellen

Door een onzer redacteuren

ROTTERDAM, 6 AUG. Het aftappen van openbare telefooncellen door de politie komt voor in gevallen van zware criminaliteit, zoals drugshandel, overvallen en ...

... betreffende telefoon.

Bekend is dat in de ontvoeringszaken van Gerrit-Jan Heijn en Valerie Albada Jelgersma cellen zijn afgetapt. Verscheidene advocaten kennen zaken uit hun ...

'Afluisteren advocaten onduldbaar'

Door een onzer redacteuren

DEN HAAG, 27 april — Het afluisteren door justitie van de telefoons van advocaten is ontoelaatbaar en in strijd met de rechten van de mens.

Deze uitspraak doet de Hoge Raad, nadat de procureur-gene-

Afluisteren

Alexander Graham Bell kon er tijdens de eerste telefoongesprekken nog van uitgaan dat ze door niemand werden afgeluisterd. Sindsdien is er heel wat veranderd. Dit artikel geeft een incompleet overzicht van het afluisteren in Nederland.

Wie luisteren af?

Justitie en Politie

In 1982 werden er in 869 zaken telefoons getapt door de politie. In 1991 werd er in 2071 zaken afgeluisterd. Ook de inlichtingendiensten, zo wordt gefluisterd, richten zich meer en meer op het afluisteren van telecommunicatie. Afluisteren is al jaren lang een 'booming business'.

In Nederland is het afluisteren van telefoongesprekken of andere telecommunicatie bij de wet geregeld. De politie mag alleen afluisteren nadat ze daarvoor toestemming heeft gekregen van een rechter-commisaris, en de inlichtingendiensten staan, althans op papier, onder controle van regering en parlement. Het is de bedoeling dat de politie alleen telefoons afluistert als andere opsporingsmethoden niet werken, of grote nadelen hebben. De rechter commissaris geeft meestal een toestemming om een aantal telefoonlijnen van een groep verdachten af te luisteren. Het aantal werkelijk afgeluisterde telefoons is dus vele malen hoger dan het getal in de vorige alinea.

Er is trouwens ook een aantal gevallen bekend waarin de politie zich niet kon inhouden en begon met afluisteren voordat de toestemming werd verkregen. Kennelijk vragen de betrokken PTT-werknemers niet altijd naar de papieren...

Juist omdat het afluisteren zo'n grote vlucht heeft genomen begint de effectiviteit van dit 'wondermiddel' af te nemen. Criminelen weten donders goed dat hun telefoon afgeluisterd kan worden en denken dus wel drie keer na voor ze belastende dingen over de telefoon zeggen.

Er gaan geruchten als zouden de diverse politiekorpsen hun afluisterpraktijken willen centraliseren. Eén landelijk afluistercentrum dat (liefst zonder medewerking van de PTT) alles kan afluisteren zou de droom zijn. Nu we allemaal mooie moderne centrales hebben is de techniek in ieder geval al lang aanwezig. Als alle informatie al als bits en bytes over een glasvezelnetwerk raast is het aanbrengen van een fysieke tap immers niet meer nodig, alleen de juiste software moet op de centrale worden geinstalleerd.

Inlichtingendiensten

De BVD heeft geen toestemming nodig van de rechter-commissaris, maar in plaats daarvan de paraaf van de premier en van de minsters van Binnenlandse Zaken, Justitie en van Verkeer en Waterstaat.

Ook houden de Inlichtingen Dienst Buitenland en de Marine Inlichtingen Dienst (Marid) zich bezig met afluisteractiviteiten, maar die zouden zich beperken tot het afluisteren van buitenlandse ambassades in Den Haag. Op het marinecomplex Kattenburg in Amsterdam zou een high-tech afluistercentrum zijn gevestigd.

Hoewel niet typisch een Nederlandse aangelegenheid is het wellicht van belang dat de V.S. een inlichtingendienst hebben die zich speciaal richt op telecommunicatie van, naar en buiten de V.S. Deze dienst heet NSA (National Security Agency).

Hoewel het oprichtings-charter van de NSA het afluisteren van Amerikanen expliciet verbiedt (de NSA was bedoeld als externe inlichtingendienst) luisterde men tijdens de Vietnamoorlog mee met de gesprekken van vredesactivisten als Jane Fonda en Dr. Benjamin Spock.

Anderen

Ook buiten de sfeer van de overheid wordt afgeluisterd bij het leven. De post legt het steeds vaker af tegen telefoongesprek, fax en datakontakt. Wie de telecommunicatie van zijn tegenstanders kan afluisteren zit op rozen. Bij industrieele spionage, ruzies tussen criminelen of echtelijk wantrouwen, speelt het afluisteren van telefoons nog al eens een rol.

Hoe luisteren ze af?

Politietaps

Een politietap werkt technisch als volgt: Na het verkrijgen van de justitiële toestemming wordt op de telefoonlijn van de verdachte een extra paar draden geplaatst. Deze draden verbinden de lijn vanaf het kabelrek in de centrale naar apparatuur die elders in het gebouw staat opgesteld. Daar wordt de audio door middel van speciale apparatuur omgevormd en via een andere lijn doorgestuurd naar de tapkamer van de politie. In die tapkamer staan recorders die lange opnamen kunnen maken, bijvoorbeeld zes uur op één kant van een C120 cassette. Deze moederbanden worden uitgetikt, en vervolgens bewaard om eventueel als aanvullend bewijsmateriaal te dienen.

De omvorming van het geluid, en het feit dat de omvormapparatuur in een andere ruimte staat dan de andere apparatuur van de PTT geven iets belangrijks aan: de PTT vertrouwt haar eigen mensen niet en wil de groep mensen die criminelen zou kunnen tippen zo klein mogelijk houden. De omvorming gebeurt door het geluid van een 3000 Hz toon af te trekken. Als de lijn van de verdachte niet in gebruik is wordt deze zelfde toon op de lijn naar de politie gezet om aan te geven dat de recorder gestopt kan worden.

Voor het aansluiten van de taps heeft de PTT in elk district een heel klein groepje speciaal geselecteerde mensen. Deze mensen hoeven alleen aan de directeur van het district verantwoording af te leggen.

I spy

Hoewel er niks officiëels bekend is over de techniek achter een BVD tap kunnen we aannemen dat de BVD door dezelfde groep mensen 'geholpen' wordt. Ook de BVD heeft ongetwijfeld een tapkamer met recorders en typistes om de afgeluisterde gesprekken uit te tikken.

In Amerika is redelijk veel bekend over de werkwijze van de communicatie-inlichtendienst NSA. Het blijkt dat deze lieden al sinds de jaren zestig en zeventig hele delen van het telecommunicatienetwerk afluisteren. Straal- en satellietverbindingen zijn met dure, grote antennes nog wel een stuk naast het doel te ontvangen. Daar grote grondstations vaak duizenden of zelfs tienduizenden gesprekken tegelijk afwikkelen kun je met een klein aantal goed geplaatste antennes een hoop gesprekken, telexen, faxen en wat al niet meer afluisteren.

Voordat een gesprek begint vindt er communicatie plaats tussen de twee centrales zodat de ontvangende kant weet waar het gesprek naar toe moet. Als je dit opvangt en vergelijkt met een 'watch-list', waarop alle telefoonnummers staan van mensen met wier gesprekken je wilt meeluisteren, dan hou je nog maar een klein gedeelte van de hele stroom gesprekken over om werkelijk te beluisteren. Toch nog een hoop mensenwerk, en misschien had de NSA daarom in 1978 al 68.203 mensen in dienst.

Met dataverkeer (fax, telex, telegrammen, computers) is het allemaal nog veel gemakkelijker: met behulp van computers zoeken naar bepaalde woorden of zinssneden die van belang zijn en alles wat 'op de zeef blijft liggen' doorsluizen voor controle door medewerkers. Omdat de NSA verklaart 'altijd 5 jaar op de state-of-the-art vooruit te lopen', is het waarschijnlijk dat men daar inmiddels betrouwbaar sprekeronafhankelijk woorden uit een telefoongesprek kan filteren. Als dat zo is kan bij telefoongesprekken dezelfde techniek worden toegepast als bij al het dataverkeer. Bezig in onschuldige gesprekken dus nooit

woorden als "Libya", "President", "Assassinate", "Bomb", "Nuclear" of iets dergelijks.

En de kleine man?

Ook zonder vergunning of megabudget kun je nog heel wat beginnen als je iemand wilt afluisteren. Je kunt de lijn te pakken krijgen door in één van de woningen te komen waar de lijn doorheen loopt en een zendertje plaatsen. Ook kun je het PTT-kastje op de hoek van de straat openbreken (of een sleutel van hebben). Dan kun je nog PTTers omkopen of gewoon een centrale binnenlopen. Ook het aanbrengen van een afluisterzendertje in de kamer waar het gesprek wordt gevoerd levert in ieder geval één kant van de conversatie op. Met richtmicrofoons kunnen vooral 's zomers (als de ramen open staan) goede resultaten worden behaald.

Radioverbindingen

Tot nu toe hebben we het alleen maar gehad over het kabelnetwerk. Het ligt voor de hand dat van echte bescherming van privacy bij een gesprek over een radioverbinding helemaal geen sprake is.

ATF1, ATF2 en ATF3

Nederland heeft op het moment drie autotelefoonnetten. Als je een scanner hebt kun je zeer makkelijk de gesprekken op alledrie deze netten afluisteren. Elk autotelefoonnet heeft twee series frequenties. De ene serie wordt gebruikt als zendfrequentie voor de steunzenders van het netwerk, de andere voor de autotelefoons. Gesprekken zijn dus full-duplex, je kunt praten en luisteren tegelijkertijd.

De steunzenders van het netwerk zijn natuurlijk veel beter te ontvangen dan de autotelefoons zelf. Je hebt dus theoretisch maar één kant van het gesprek. Gelukkig zorgt 'overspraak' in de gebruikte autotelefoons en de gewone telefoons aan de andere kant van de lijn er voor dat er altijd wel een beetje van het geluid van de autotelefoonabonnee doorheen komt.

Als je wilt luisteren naar ATF1 kun je de steunzenders ontvangen tussen de 153.01 en 153.75 MHz. De autotelefoons zelf zitten altijd 4.6 MHz lager dan de steunzender, dus

Zaak tegen autoschutter aangehouden

ZWOLLE, woensdag
De rechtbank in Zwolle heeft gisteren de strafzaak tegen de 30-jarige R.O.B. uit Amsterdam aangehouden tot 29 september. B. wordt ervan verdacht op 27 maart van dit jaar vanuit zijn auto meermalen op een ander voertuig te hebben geschoten.

Dit gebeurde na een incident tussen de beide bestuurders waarbij B. de achtervolging zou hebben ingezet en er met snelheden van 160 kilometer per uur over de A1 gereden werd.

De Amsterdammer heeft steeds ontkend dat hij geschoten heeft. Een familielid, dat hij niet met name wil noemen, zou in zijn auto hebben gereden. Dit familie-lid had volgens de verdachte zijn auto geleend en zou daarom per auto-telefoon hebben verzocht.

Daarom wil de rechtbank als getuige-deskundige een medewerker van PTT-Telecom horen over de auto-telefoonnetten op het traject Muiden-Zeewolde. Van dit net is slechts één net onderzocht op gesprekskenmerken. De rechtbank wil weten, hoe het met de twee andere netten is gesteld.

Verder zal op 29 september een medewerker van het gerechtelijk laboratorium worden gehoord. Deze man heeft zich bezig gehouden met het technisch onderzoek. De officier van justitie had op 28 augustus drie jaar cel geëist. (ANP)

tussen 148.41 en 149.15 MHz. Op ATF1 zijn de steunzenders continu in de lucht met een datariedel waar veel scanners zonder speciale aanpassingen op blijven 'hangen'. Wel weet je zeker dat je het hele gesprek kan meeluisteren: er wordt tijdens het gesprek niet van kanaal naar kanaal geschakeld.

Bij ATF2 zitten de steunzenders tussen 461.31 en 465.73 MHz, en de autotelefoons tussen de 451.31 en 455.73.

Bij ATF3 zitten de steunzenders tussen 935.0125 en 959.0000 MHz, de autotelefoons tussen 890.0125 en 914.0000 MHz. Gesprekken op ATF2 en ATF3 kunnen zoals gezegd van de ene steunzender naar de andere verplaatst worden, en dan verwisselt over het algemeen ook het kanaal waarop gezonden wordt. Bij ATF3 gebeurt dit nog iets vaker dan bij ATF2, omdat er meer steunzenders zijn en de autotelefoons over het algemeen over minder zendvermogen beschikken.

Dit is allemaal hele simpele informatie die bruikbaar is als je met je scanner zelf naar gesprekken van anderen zou willen luisteren. Er zijn veel spookachtigere zaken te doen. Zo zou je een ontvanger aan je computer kunnen hangen die gericht gesprekken van of naar een bepaalde autotelefoon afluistert. Ook kun je op deze manier een databank opbouwen van alle autotelefoonverkeer in de delen van het netwerk die vanuit je huis te ontvangen zijn. Dat is vaak meer dan je denkt, als je tenminste gebruik maakt van richtantenne's. Hier op ons redaktiekantoor in de Bijlmer zou je zonder al te veel moeite alle autotelefonie rond Amsterdam en Utrecht op kunnen pikken. De regering wil het opzetten van 'bijzondere ontvanginrichtingen', zoals een netwerk van ontvangers voor autotelefonie, graag verbieden. De wet die ze daarvoor bedacht hebben maakt echter een uitzondering voor de BVD. Raad eens wie er waarschijnlijk al sinds jaar en dag zo'n netwerk heeft?

Er komen steeds meer steunzenders voor ATF2 en ATF3. Dit betekent dat de computers die het netwerk besturen met steeds meer precisie weten waar alle abonnees uithangen. Zodra je namelijk je telefoon aanzet meldt die zich aan bij het netwerk. Zodra contact met de steunzender verloren wordt zoekt de telefoon zelf een nieuwe steunzender. De politie begint er, volgens onze bronnen binnen de PTT, langzaam achter te komen dat ze een hoop kosten kunnen besparen als ze gewoon aan het autotelefoonnet vragen waar de gehele nederlandse topcriminaliteit zich bevindt. Je leest het goed: plaatsbepaling van alle autotelefoonabonnees is mogelijk, en nog volledig legaal ook!

We geloven niet zo veel van het in de pers breed uitgemeten verhaal dat politie en PTT technische moeilijkheden zouden hebben bij het afluisteren van autotelefoons. De techniek maakt het volgens ons prima mogelijk om bepaalde autotelefoons af te luisteren. En als er dan toch problemen zijn met het afluisteren van autotelefoons dan zouden ze dat volgens ons wel voor zich houden. Criminelen worden aangemoedigd om toch vooral een autotelefoon te nemen. Handig en niet af te luisteren.

Kermit

De PTT levert ook de Kermit zaktelefoon. Het kontakt tussen de Kermit telefoon en de vaste basisstations verloopt geheel digitaal. Weer is er voor de scannerfreak niks af te luisteren. Het wordt gebracht als de nieuwe telefooncel in je borstzak: Met je Kermit bellen bij een Greenpoint. Een belangrijk aspect van het bellen in een telefooncel is echter verdwenen: het netwerk houdt bij wie er wanneer met wie belt.

Selectief afluisteren van een bepaalde Kermit telefoon is waarschijnlijk voorlopig nog wel even moeilijk, maar als straks alle Greenpoints via snelle digitale lijnen met de centrale verbonden zijn, is ook dit geen probleem meer.

Draadloze telefoons

Heb je in allerlei soorten en maten. Natuurlijk kun je alle analoge modellen gewoon met een scanner afluisteren. Grappig

is dat in de V.S. het afluisteren van draadloze telefoons legaal is, terwijl het afluisteren van autotelefoons een misdrijf is. In een volgende Tic zullen we proberen een overzicht van gebruikte frequenties en dergelijke te geven.

Semafoons

We hebben het er in vorige Hack-Tics vaak genoeg over gehad: semafoonoproepen zijn zeer gemakkelijk te onderscheppen. Lees Hack-Tic 14/15 voor alle technische gegevens. Het 'leuke' is dat iedere amateur het kan betalen om behoorlijk geavanceerde dingen te doen.

Het leuke van het semafoonnet is dat het afluisteren veel democratischer is: iedereen kan zonder al te veel geld en moeite alle gegevens bemachtigen. Als er straks een Europees semafoonnet komt is wel de vraag wie er dan allemaal kan meekijken met oproepen van en naar personen in Nederland.

Tegenmaatregelen

Early warning

Op de hacker-bbs'en duikt elk half jaar wel iemand op die een methode heeft om te weten te komen of je wordt afgeluisterd. Zo kun je bellen naar bepaalde nummers in Amerika die een ononderbroken stijgende pieptoon geven. Als er gaten in die toon vallen zou je telefoon worden afgeluisterd. Deze nummers bestaan (zie Hack-Tic 8), maar ze zijn slechts bedoeld als test voor de Amerikaanse PTT. Onderbrekingen duiden op filters in het internationale deel van de lijn (overigens wel interessant, maar dat heeft niks met afluisteren te maken, zie Hack-Tic 13).

Ook zou, als je een afgeluisterde lijn vanuit een telefooncel belt, het kwartje vallen nog voordat er wordt opgenomen. Wie dat bedacht heeft weten we niet, maar een appeltaart krijg je er niet voor.

Dan zijn er nog gecompliceerde apparaten die de lijn-impedantie meten en veranderingen (zoals een aftakking op de hoofverdeler) vaststellen. Duur en niet 100% effectief (wat als je lijn al afgeluisterd werd voordat je de eerste meting deed ?). En als je digitaal wordt getapt is er op de lijn al helemaal niets meer van te meten.

Versleuteling ?

Je zou de spraak kunnen versleutelen. Hiervoor is commercieel al een groot aantal apparaten op de markt. De meeste apparaten zijn erg duur (vele duizenden guldens). Zelfs als je zo'n apparaat aanschaft blijft de vraag: "Vertrouw ik de leverancier?". De eventueel meeluisterende amateur of opsporingsambtenaar is wellicht ontmoedigd. Maar wie zegt bijvoorbeeld dat er geen achterdeurtje in zit voor inlichtingendiensten?

Er is op dit moment in Amerika al een gevecht gaande rond coderingsalgoritmen. Een groep senatoren wil cryptografie voor burgers alleen toestaan als ze de sleutel registreren bij de overheid, en mensen dus het recht ontnemen om hun berichten op een doeltreffende manier tegen de overheid af te schermen.

Een groot aantal mensen vertrouwt voor de opslag van gegevens op computeragenda's met een wachtwoord. Het is van een aantal merken computer-agenda's bekend dat er achterdeuren inzitten en dat de fabrikanten voor justitie graag een print-out van alle gegevens maken. Waarom zouden de makers van spraakversleutelingsapparatuur niet een zelfde 'deal' hebben? Nu processors sneller en goedkoper worden is het wachten op iemand die een public domain spraakversleutelingsmethode bouwt.

Verkeersanalyse

Ook als je alle gesprekken codeert is er voor de afluisteraars uit het patroon van de verbindingen nog wel het een en ander af te leiden. Wie praat wanneer, hoe lang en met wie. Ook kunnen afwijkingen op een normaal belgedrag worden vastgesteld. Bij mensen die gebeld worden kan weer zo'n zelfde analyse worden gedaan totdat een

heel contactnetwerk opduikt. Alle analyse die zich niet met de inhoud van de communicatie bezighoudt noemt men 'verkeersanalyse'. Iets verderop in dit artikel staan een paar leuke bedreigende voorbeelden.

In deze tijd van digitale centrales is het tamelijk makkelijk om aan de gegevens te komen die voor verkeersanalyse nodig zijn. Het feit dat de PTT deze gegevens nog een tijdje bewaart betekent dat je een analyse van een hele groep mensen ook met terugwerkende kracht kunt doen.

Stel: om telefoonkosten af te kunnen trekken van de inkomstenbelasting wordt in de toekomst een gespecificeerde nota gevraagd. Journalisten bellen met geheime bronnen. De belastingdienst is een overheidsdienst, en bewaart alle papieren jarenlang. Dus zelfs als de PTT de gegevens niet bewaart kan een geheime dienst of overijverige politieambtenaar achter de bronnen van deze hypothetische journalist komen.

Stel: je hebt een file met alle semafoonoproepen van de laatste 5 jaar.

Scenario 1: Kijk wie er allemaal oproepen plaatsen naar persoon X. Je hebt dan een lijst met telefoonnummers (de meeste mensen geven hun eigen nummer door). Ga dan terug in de file en zoek uit welke mensen er nog meer gepiept zijn door deze mensen. Zoek van deze piepers weer uit wie er verder nog naartoe gepiept hebben. Binnen een paar uur rekenen heb je een kant en klaar organisatieschema van de hele organisatie waar persoon X deel van uitmaakt.

Scenario 2: Geef de computer een lijst met alle kernongelukken in Europa in die 5 jaar en de computer geeft je alle niet gepubliceerde ongelukken en bijna-ongelukken omdat ruwweg dezelfde mensen opgepiept werden.

Conclusie

Als je de techniek achter de schermen kunt en wilt snappen kun je je communicatie (bijvoorbeeld door middel van cryptografie of cryptofonie) redelijk afschermen tegen al te nieuwsgierige oren en ogen. Waterdicht is het nooit: wie de technologie beheerst kan zich met veel moeite altijd een beeld vormen van waar je mee bezig bent.

Ideaal zou zijn om cryptofonie standaard in elke telefoon te bouwen; geheel transparant in gebruik, dus zonder dat het moeite kost om het te gebruiken. De slechterikken gebruiken het over een paar jaar toch allemaal, dus waarom dan niet iedereen? Cryptofonie wordt pas goedkoop als veel mensen het hebben.

Er zou bij het ontwerp van telecom-netwerken over de privacy-aspecten moeten worden nagedacht. Telefooncentrales worden over het algemeen gebouwd om 20 jaar mee te gaan: misschien vertrouw je de regering van nu, maar wie vertrouwt de regering van 2012?

Het duurt over het algemeen wel een tijdje voordat de overheid door heeft wat voor vergaande mogelijkheden de nieuwe techniek heeft, maar als ze het eenmaal doorhebben gebruiken ze het ook, zelfs als dat wettelijk helemaal niet mag. Omdat er bij het aan de gang houden van het telefoonnet steeds minder mensen betrokken zijn wordt het ook steeds makkelijker om omvangrijke zaken geheim te houden.

Rop



De toekomst van het hacken

We stuurden 5 bekende en minder bekende hackers een lijstje vragen. Uit hun antwoorden blijkt dat deze hackers er zeer verschillende denkbeelden op na houden over onder andere de toekomst van het hacken en de gevolgen van de recente arrestaties. Omdat het niet terzake doet wie ze zijn, en omdat we dachten dat het wellicht de eerlijkheid ten goede komt geven we ze de nummers 1 tot en met 5.

HT: Wat is hacken voor jou?

1: Hacken is voor mij ontdekken. Het ontdekken van een nieuwe wereld, het netwerk, computersystemen, mensen. Hacken is reizen, speuren & hard werken. Hacken is voor mij ook net zo lang doorgaan met een probleem, totdat je er een oplossing voor hebt. Hacken hoeft wat dat betreft niet eens wat met computers te maken te hebben, meer met het creatief en op originele manier oplossen van problemen.

2: Ehm, een sport, een hobby, een uitdaging, een beetje van alle drie.

3: Een hobby, mijn drang om alles te weten te komen over netwerken, operating systems wat er te weten valt, dieper te gaan dan een gewone burgerman doet. Techniek manipuleren zodat het doet wat jij wil (phreaken en zo dus ook)

4: Hacken is handig zijn, niet kraken en vernielen, maar slim programmeren.

5: Leuk.

HT: Waarom hack je?

1: Je vraagt aan de melkboer toch ook niet waarom 'ie melk verkoopt?

2: 'Because it's there', hahaha. Ik hack vanwege de spanning, de uitdaging, omdat ik het reuze interessant vindt om op grote computers rond te hangen en omdat ik geen andere manier had om usenet-NEWS te lezen :-) En ik hack omdat ik nieuwsgierig ben.

3: Omdat ik het niet laten kan. De hele dag een computer alleen maar gebruiken voor 'nuttige' dingen zoals 'wp' gebruiken, of vage numerieke berekeningen. Soms moet het, maar ik hou dat nooit zo lang vol, dan ga ik weer interessante netwerk utilities schrijven.

4: Omdat ik mijn programma's en ideeen wil testen, daarvoor moet ik ze kunnen testen op machines met een netwerkaansluiting, die ik zelf niet heb, dus moet ik wel op andermans machine gaan testen.

5: Voor de sport.

HT: Wat klopt er wel en niet aan het beeld dat mensen van hackers hebben?

1: Er klopt over het algemeen zeer weinig van het beeld dat de media schetsen van hackers. Hackers worden afgeschilderd als parasieten, vernielers, inbrekers etcetera. Het beeld dat mensen hebben van hackers is natuurlijk totaal vertekend door het lawaai van de sensatie. Het is ook jammer dat hackers worden gezien als een gevaar voor de samenleving, omdat we de macht hebben om netwerken op bepaalde punten plat te leggen, zogenaamd techno-terrorisme, zoals de CRI dat zo mooi noemt.

Waar iedereen bang voor is zijn niet de hackers, maar criminelen die informatie stelen om die voor hun eigen gewin te gebruiken. Dat is totaal tegen de filosofie van het hacken. Hacken is wat dat betreft het tegenovergestelde, hackers bewijzen het volk juist een dienst door te laten zien hoe kwetsbaar de systemen zijn waar hun belastingzaken of andere intieme informatie zijn opgeslagen. Een hacker zal zijn informatie niet verkopen, noch gebruiken terwille van zijn eigenbelang. Hackers zijn inventief en creatief genoeg om op andere 'legale' manieren hun brood te verdienen.

Het is ook heel jammer dat een aantal 'hackers' systemen heeft vernield, of moedwillig mensen heeft getreiterd. Dat heeft niet

echt bijgedragen aan de goodwill tussen hackers en systeembeheer. Dit is voor veel systeembeheerders natuurlijk wel een reden om hackers af te schilderen als demonen van het netwerk.

2: Meestal geen zak. Voornamelijk dankzij de media, die de hacker afbeelden als crimineel, iemand die snuffelt in andermans gegevens, een etter die het leuk vindt om computers te laten crashen. Gelul natuurlijk, maar sommige hackers van de nieuwe generatie denken dat ze zich zo moeten gedragen, en dus kan de media straks gaan schreeuwen "zie je wel!", en is de cirkel weer rond. Waar ik ook niet goed van word, is dat ze (de media) de computer gaan vergelijken met een huis. Gelul, in een computer woon je niet, en de computers waar ik in zit/zat waren computers van een groot bedrijf. Als je de computer dan toch met een gebouw moet vergelijken, vergelijk het dan maar met een station. En de hackers met jongens die 's nachts stiekum over de rails heen lopen en de treinen van binnen bekijken omdat ze gek op treinen zijn.. of met een bibliotheek, en de hackers met mensen die stiekum 's nachts boeken gaan lezen.

3: Hangt er van af welk beeld van welke mensen je bedoeld, maar het beeld van de 'mad hackers key party', of van de voor vernieling en oplichting gearresteerde hacker (die dus kennelijk vernield en opgelicht heeft) klopt in ieder geval niet. Dat van de Robin Hood van het netwerk vind ik ook een beetje onzin. Ik ben gewoon iemand die erg geinterresseert is in netwerken, en ik zie het als een uitdaging om dingen voor andere doeleinden te gebruiken dan ze bedoeld zijn.

4: Het beeld dat hackers bugs vinden, aan de beheerder mailen en dan een baan/usercode krijgen. Meestal zijn crackers dom, wissen/beschadigen ze files, gooien de machine plat, maar vinden nooit iets nieuws. En als je al naar de sysop mailt, wordt je eraf gegooid, ze zijn nooit dankbaar.

5: Als mensen het woord 'hacken' horen denken ze meteen aan het overboeken van astronomische bedragen naar een bankrekening in Zwitserland. Bullshit natuurlijk.

HT: Hoe zie je hacken in de toekomst?

1: Door de negatieve ontwikkelingen m.b.t. de wet tegen computercriminaliteit, en de twee zaken waarin hackers zijn gearresteerd, denk ik dat hackers op een andere manier hun creativiteit gaan uiten. Het is toch triest dat mensen nu de mogelijkheid is ontnomen om vrij over het net te reizen, zonder belemmeringen. Als je echt nog een systeem in wilt, bijvoorbeeld om te laten zien hoe slecht het is beveiligd, is het nu zaak om erg voorzichtig te werk te gaan.

2: Hacken gaat zeker veranderen. Waarschijnlijk wordt het hacken harder, een mentaliteit van "jullie zijn niet aardig tegen ons, dan zijn wij ook niet aardig tegen jullie". En hup, dan word de hele disk gewist. Waarschijnlijk gaan de hackers ook minder in grote groepen werken, meer ondergronds, vaker gebruik maken van encryptie, etc etc. Binnenkort zal er bijna nergens op schijf nog een un-encrypted logfile van een hack te vinden zijn. Ook zullen hackers meer met hardware te maken krijgen, en dus zullen ze meer samen gaan werken met technophreaks.

3: Ik denk niet dat hackers zullen ophouden met bestaan door hard overheidsbeleid, maar wel meer underground dan tot nu toe

4: Direct bellen met de telefoon wordt onmogelijk, er zullen meer truuks bedacht moeten worden. Meer beginners, die bijv. nieuwe internet-dialins voor de mensen die weten wat ze doen verpesten, door dom te gaan inloggen om passwords te testen, met root/root, guest/guest, test/test, met de milnet lijst van hacktic in de hand. Met teveel hackers blijven er niet genoeg machines/resources over voor de experts.

5: Geen idee. Voorlopig zal er wel niet veel veranderen denk ik.

HT: Wanneer ben je begonnen? Is er sinds die tijd veel veranderd? Ben jij veranderd?

1: Ik ben zo'n jaar of 3 geleden begonnen, in die tijd zijn de veranderingen

stormachtig geweest. Hacken in Nederland is wat intensiteit betreft echt heel erg afgenomen. 2 1/2 jaar geleden waren er voor iedereen mogelijkheden, nu heb ik een beetje het idee dat alleen de 'inner circle' nog actief is. Het is ook zo dat systemen steeds beter worden beveiligd, dus het is moeilijker om erin te komen als beginnende hacker. Voor de toekomst zie ik het nog somberder in dan het nu al is, door de ogenschijnlijk harde aanpak zullen steeds minder mensen zich in het diepe wagen. Voor mij is dit een reden om de faciliteiten die je tot je beschikking hebt als hacker, op een andere manier beschikbaar te stellen aan mensen die daar interesse in hebben. We moeten er voor zorgen dat het netwerk niet voor een kleine elite is, maar voor iedereen die behoefte heeft om erop rond te reizen.

2: Pffff. Ik ben geloof ik begonnen in 1988 of zo. Maar echt flink bezig ging ik pas later, toen ik op THIS andere hackers tegenkwam. Daarvoor was ik meestal maar in mijn eentje bezig. Mijn eerste hack was een UNIX, ik geloof van ALCATEL. Ik wist toen nog bijna niets van UNIX, maar vond het wel erg interessant. Hacken is erg veranderd (vooral de laatste tijd). In het begin was het een grote broederschap, iedereen deelde wat er gevonden werd. Later was het onderling wantrouwen groter en vormden zich kleine groepjes. Ik ben door het hacken zelf wel veranderd: nog gekker geworden dan ik al was, en je leert er de meest vreemde mensen kennen. Ik heb nu ook minder vertrouwen in de media en politici dan voorheen, je wordt wat wantrouwiger. (Niet dat ik ooit veel vertrouwen in politici heb gehad)

3: Ik ben echt begonnen met hacken vlak nadat ik m'n eigen modem kreeg, ergens december 1989. Daarvoor had ik wel eens wat met allerlei terminalservers van universiteiten gespeeld, maar nooit echt iets bereikt.

Ja, er is veel veranderd, nu wordt er vanuit systeembeheerderskant hier in Nederland veel sneller gereageerd. Ook zijn er duidelijk oude en nieuwe hackers. Dingen als de tymnet-chat parties, of chatten op qsd, altos etc... komt niet meer voor. Ik weet nu veeeeeeeeel meer over unix, ethernet, Novell, VMS, ... dan vroeger.

4: Ik hack sinds 1988. Ja, er is veel veranderd.

5: Zo'n 2 à 3 jaar geleden. De systemen zijn nu nog steeds even slecht beveiligd als toen, alleen heb ik veel meer verstand van die systemen gekregen. Dus het hacken wordt steeds gemakkelijker.

HT: Bang om gepakt te worden?

1: Nee, niet echt, ik neem (meestal:-) geen onnodige risicos. Ik heb me er wel een tijdje druk over gemaakt, nu helemaal niet meer.

2: Nu niet, maar ik heb wel mijn vlagen van paranoia gehad (disks verbranden, papier versnipperen en verbranden etc.). Maar zoals een beroemd iemand al eens gezegd heeft : "mij pakken ze nooit".

3: Niet echt, ik ben wel geschrokken, nadat ik hoorde wat voor maatregelen men wilde nemen tegen 'de hacker'

4: Niet meer :-)

5: Ach, toen niet en nu nog steeds niet.

HT: Zou je kunnen stoppen met hacken? Heb je het wel eens overwogen?

1: Ligt eraan wat je onder hacken verstaat. Het laatste jaar gebruik ik alleen nog mijn eigen accounts, als dat is wat met de vraag bedoeld werd. :)

2: Yep, helemaal stoppen nooit, maar ik was al voor een groot deel gestopt voor de 'grote klap'. Ik had andere interesses gekregen (o.a. phreaking, haha), en ik kwam tijd tekort. <zeik-mode AAN> Verder was het vroeger leuker, toen kon je nog eens een login met iemand delen. Tegenwoordig geef je een login weg, om er later achter te komen dat honderden amiga-kids er volop gebruik van maken. <zeik-mode UIT>

3: Nee, nee.

4: Ik ben nu gestopt, dwz. ik hack niet meer, maar ik verzin nog wel truuks, ik schrijf programma's, die laat ik door anderen gebruiken.

5: Ik ben momenteel gestopt. (Ik doe nog

wel eens wat, maar nooit vanuit thuis en het blijft ook bij een beetje "prutsen").

HT: Hoe ga je voorkomen dat je gepakt wordt?

1: Ik probeer, zoals ik al zei, geen onnodige risico's te nemen.

2: Hah, ALS ik wat ga doen, doe ik het vanaf een veilige plek, dus een telefooncel, iemand anders' lijn (PTT of zo), of een gepliekte lijn. Verder houd ik lekker mijn klep dicht tegen mijn omgeving, en crypt ik mijn hele HD.

3: Voorzichtig zijn, terminalzalen van willekeurige universiteiten zijn wel een geschikte plek momenteel.

4: Niet meer zelf hacken.

5: Door als ik hack niet meer vanuit thuis te werken.

HT: Wat doe je als je gepakt wordt? Stop je daarna?

1: Geen idee. Veel lawaai maken lijkt me een prima idee. Stoppen ? Nee, dat zou niet echt een reden zijn, als ik gepakt wordt lijkt me dat juist een reden om door te gaan. Echt goed kan ik er natuurlijk niet over oordelen, zolang het me niet is overkomen.

2: Als ik gepakt word, krijg ik last van een acute geheugenstoornis. Of ik daarna stop, weet ik nu nog niet. Waarschijnlijk niet, want ik heb dan toch weinig meer te verliezen.

3: Tja, schrikken denk ik, niks zeggen, hopen dat ik tegen die tijd alles netjes gediskreet op mijn HD heb staan. Misschien even, maar ik denk niet dat ik het kan laten.

4: Ja.

5: Momenteel dus bijna wel ja.

HT: Zie je hacken als 'fout'? Definieer goed en slecht in relatie tot hacken.

1: Een goede definitie van 'het goede' en 'het kwade' is te vinden in de Ilias & de Odysee van Homerus :-) Goed en slecht zijn niet definieerbaar, en hebben voor elk mens een andere betekenis, veelal bepaald door de cultuur en levensomstandigheden. Moorden is slecht, daar is iedereen het over eens, maar als je als soldaat in dienst van het 'Vaderland' een massamoordenaar bent, krijg je een medaille. Ik begrijp niets van goed en slecht, en ben dus niet de persoon die daar antwoord op kan geven. Wat me te ver zou gaan is om iemand die informatie steelt en doorverkoopt, een 'goede' hacker te noemen. Zo iemand is helemaal geen hacker.. Conclusie, er zijn geen 'slechte' hackers.

2: Non, hacken op zich zie ik zeker niet als fout. Wat er met de gehackte systemen gedaan wordt kan echter wel fout zijn: disks wissen, systeem crashen, etc. zie ik als slecht. Je kunt hacken vergelijken met zelf vuurwerk maken: als je er alleen maar rotjes van maakt, en die op een stil plekje afsteekt, omdat je zo van knallen houdt, is dat niet slecht. Als je bommen maakt, en er een huis mee opblaast, dan is dan wel slecht.

3: Nee, maar het hangt af van de manier, je gedrag binnen een computer en je doeleinden. Iemand die ergens binnenkomt, en vervolgens de boel begint te slopen is echt fout bezig, maar simpele om hacktechnische redenen toegepaste veranderingen aan files (logfiles, dingen als .rhosts, trojans ...) veroorzaken geen schade. Zodra hacken economisch gewin tot gevolg heeft, is het ook een foute boel. (.... Amigakids die phreak trucs verkopen). Met het doorkijken van prive dingen van mensen heb ik geen problemen als je maar geen gebruik van de verkregen informatie maakt. Als je dat doet pak je daar onschuldige mensen mee.

4: Het beeld dat hackers recht hebben op root access in milnet computers is dubieus, evenals het idee dat de PTT crimineel is door niet alle *-diensten aan te bieden, het is jammer, maar niet verplicht voor de PTT om alles te doen wat het publiek vraagt en geen geld oplevert. Maar de manier waarop hacken fout wordt genoemd is zwaar overdreven.

5: Ik zie hacken om het hacken niet als fout. Pas wanneer er gegevens waar mensen wat aan hebben (dus geen logfiles ed) vernietigd worden of andere gebruikers veel last van je hebben (afgezien van de systeembeheerder die toch altijd denkt last van je te hebben) vind ik dat je verkeerd bezig bent.

Uitslag lezersenquete

In de vorige Hack-Tic zat een kaart met daarop een heleboel vragen. We hebben alle binnengekomen kaarten in de computer ingevoerd. Een beeld van onze gemiddelde lezer.

Voordat we de inhoud van al deze kaarten gaan bekijken valt op dat maar liefst 55 mensen de kaart niet of onvoldoende hebben gefrankeerd, en dat dat maar in 5 gevallen tot strafport heeft geleid. Van deze mensen hebben er 13 iets mafs op de plaats geplakt waar de postzegel had moeten zitten. We zagen een Pickwick theelabeltje, een Braziliaanse postzegel, een Duckstadzegel, een lachende mevrouw uit de ECI reclame (of zoiets) en een bonnetje van slagerij Hoefsmit in Rotterdam.

Geslacht

We hadden al een donkerbruin vermoeden, maar dat het zo erg zou zijn... Als je dit leest is de kans 98.9 procent dat je een jongetje bent. Met andere woorden: Hack-Tic lezers zijn jongens en mannen. Kennelijk is de hackerwereld zelfs in vergelijking met de rest van de computerwereld nog achtergebleven gebied. We vinden het zelf een beetje jammer dat niet meer meisjes hacken, maar het zij zo.

Leeftijd

0-10	0.4%	26-30	14.7%
10-15	1.1%	30-35	9.8%
16-20	22.8%	36+	15.1%
21-25	35.1%		

Begrippen

Dan nu de vragen waarbij we jullie een lijst met begrippen voorlegden en vroegen erop te reageren met 'huh', 'o ja', 'kan ik mee omgaan' of 'kan ik dromen'.

	Huh	O ja	kan mee omgaan	Kan ik dromen
UNIX	32.6%	30.6%	27.4%	9.4%
VAX/VMS.	46.4%	29.8%	18.3%	5.5%
MS-DOS. (besturingssystemen)	5.2%	4.5%	30.2%	60.1%
Apple Mac.	39.8%	32.6%	19.6%	7.9%
Atari ST.	47.1%	28.7%	18.7%	5.5%
Amiga.	40.2%	28.3%	17.5%	14.0%
BBC/Atom.	68.4%	19.6%	8.8%	3.2%
Apple II.	59.5%	23.4%	12.6%	4.5%
Atari 8-bit.	67.4%	19.3%	10.2%	3.2%
C-64.	29.3%	20.2%	25.4%	25.1%
ZX-Spectrum.	45.6%	27.0%	17.9%	9.5%
NeXT.	73.6%	21.5%	2.8%	2.1%
Sun.	59.0%	21.8%	16.8%	2.5%
Apollo.	71.2%	18.6%	8.8%	1.4%
Archimedes. (computers)	66.4%	25.5%	5.9%	2.1%
C.	26.5%	24.7%	26.5%	22.3%
BASIC.	13.5%	12.1%	33.6%	40.8%
Clipper. (programmeertalen)	46.0%	28.8%	17.2%	8.1%
Ethernet.	41.4%	21.1%	29.1%	8.4%

TCP/IP.	64.2%	16.5%	14.0%	5.3%
X25. (netwerken)	52.7%	22.8%	18.2%	6.3%
SWR-meter. (Zendantennes)	53.5%	17.5%	14.7%	14.3%
Soldeerbout.	13.1%	11.4%	30.7%	44.8%
S-39. (soldeerflux)	49.9%	10.1%	18.1%	22.0%
74HC14. (Chip)	60.3%	8.7%	14.6%	16.4%
AK-47. (Machinegeweer)	72.7%	6.7%	8.1%	12.6%
APZ-14. (helemaal niks)	94.4%	3.9%	0.7%	1.1%
Splatmaster. (Paintball-term)	90.8%	2.8%	3.2%	3.2%
Oscilloscoop. (Meetapparaat)	24.3%	21.2%	28.5%	26.0%
rdist. (UNIX security-bug)	91.6%	5.6%	1.0%	1.7%
Dragon's Lair. (Amiga spel)	58.6%	21.4%	13.0%	7.0%
RSA. (Versleutelingsalgoritme)	81.4%	9.5%	7.0%	2.1%
DTMF. (Toontjes telefoon)	35.5%	24.9%	22.1%	17.5%
C5. (DTMF voor gevorderden)	58.3%	23.9%	13.3%	4.6%
Tempest.(o.a. afscherming monitor)	82.2%	9.8%	3.8%	4.2%
Durex.(Condooms)	19.1%	8.7%	31.6%	40.6%
Cannabis.	45.5%	17.8%	13.6%	23.1%
Geld.	29.3%	8.7%	24.4%	37.6%
Zeep.	29.3%	12.9%	35.7%	22.0%
Mensen.		25.3%	10.4%	34.3%

Vroeger, nu en later

	vroeger	nu	later
Lagere School	90.9%	0.0%	1.4%
LBO	21.8%	0.7%	2.8%
MBO	30.7%	7.3%	2.8%
HBO	14.4%	15.1%	10.5%
MAVO	33.3%	0.7%	1.8%
HAVO	24.5%	4.9%	3.1%
VWO	38.7%	6.6%	4.5%
Universiteit	18.9%	12.7%	17.5%
Computerbaan	9.7%	26.9%	30.5%
Electrobaan	8.3%	9.0%	16.3%

	vroeger	nu	later
Telecombaan	3.5%	7.0%	16.5%
Militaire dienst	17.2%	4.9%	15.8%
Politiek links	16.1%	17.3%	8.0%
Politiek rechts	6.6%	15.1%	10.9%
Baanloos	13.4%	9.7%	9.1%
Stom werk	18.4%	12.7%	5.0%
Werk bij media	4.2%	4.8%	8.3%
Eigen bedrijf	3.7%	11.3%	34.2%
Sysop	11.8%	13.7%	17.6%
De afwas	21.9%	19.9%	31.3%

Grappig detail: van de mensen die nu links zijn verwacht 14% later rechts te worden. Van de mensen die vroeger links waren noemt 25% zich nu rechts. Veel lezers vinden terecht dat wij met hun politieke gezindheid niks te maken hebben.

Ben je

	Ja	Nee
Hacker?	43.9%	44.3%
Phreak?	51.4%	38.1%
Cyberpunk?	16.8%	69.1%
Warez-dude?	11.2%	72.6%
Hardw. phreak?	45.3%	43.9%
UNIX-wizard?	10.9%	76.1%

	Ja	Nee
Data-traveller?	35.3%	51.4%
Sys.beheerder?	28.0%	59.8%
Manager?	19.3%	69.1%
Crimineel?	19.5%	66.2%
Gevaarlijk?	32.2%	53.8%
Staatsgevaarlijk?	24.8%	60.5%

Inkomen

6.2% van onze lezers heeft een zeer laag inkomen en leeft dus eigenlijk nog van zakgeld. 32.5% heeft een uitkering of studiebeurs, 34.4% vindt van zichzelf dat hij een gewoon inkomen heeft, 26.0% noemt zijn inkomen hoog, en 0.6% zit boven de ƒ100.000 per jaar

Diversen

17.1% van onze lezers heeft 1 computer, 29.5% heeft er twee, 22.8% heeft er drie, 12.6% heeft er vier, 12.6% heeft er vijf tot tien en 1.4% heeft er meer dan tien. 3.5% weet het niet of heeft geen mening. Gemiddeld heeft de Hack-Tic lezer zo'n 300 floppen. 15 procent heeft er 1000 of meer.

Gemiddeld wordt elke Hack-Tic door 2 mensen gelezen. één lezer deelde zijn Hack-Tic met 27 anderen. 15% van onze lezers draait kopietjes van de Hack-Tic, gemiddeld draaien deze kopiëerders 2 kopietjes per persoon.

Hoeveel procent van Hack-Tic snap je niet?.

0-10	48.1%	51-60	2.1%
11-20	14.7%	61-70	3.9%
21-30	7.0%	71-80	2.8%
31-40	5.6%	81-90	1.1%
41-50	10.2%	91-100	3.2%

Hoeveel uur per dag zit je achter de computer?

0	2.4%	7-8	9.8%
1-2	17.8%	9-10	12.6%
3-4	22.4%	11-12	5.2%
5-6	18.2%	13+	9.8%

77.3 procent van onze lezers heeft een modem, 50 procent betaalt kijk en luistergeld. 30 procent woont nog bij zijn ouders, 43.2 procent heeft een auto. 51% heeft wel eens een computer gekraakt. 70% heeft wel eens software gekraakt. 55% heeft wel eens getelefoneerd zonder te betalen. 22% heeft wel eens een virus geschreven. 26% leest Hack-Tic (ook) vanwege zijn werk. 52% heeft alle Hack-Tics thuis liggen.

Onze goede kanten

Veel lezers waarderen de tips en trucks, de rauwe informatie dus. Ze willen weten waar de lekken en zwakke punten zitten. Iets minder vaak werd genoemd het 'gaten schieten in de technocratie', 'het belachelijk maken van autoriteiten', 'jolig anti-techneuten karakter', 'dat de ptt altijd zo heerlijk afgezeken wordt', 'lak aan alles' etc. Dan waren er nog mensen die alles goed vinden. Iemand had het over 'maximale informatie absorbtie'. Ook de tekeningen en het logo worden meerdere malen genoemd. 'Dat het nog steeds bestaat!!!!' schreef iemand. Daar kunnen we ons wel in vinden. Iemand beschreef 'de nietjes' als het beste. Hmmpf.

En onze slechte kanten

Veel geklaag over ons onregelmatig verschijnen. Een paar klachten van mensen die vinden dat we te veel oude truuks brengen. Sommigen klagen over te veel diepgang, anderen over te weinig. Mensen ergeren zich aan de gekste dingen. Een greep: ongebruikte witte stukken, onprofessionele voorkant, de lezers en zelfs enquetes. Iemand verweet ons 'lullige geintjes over het geloof' en iemand anders vindt ons maar 'eigengereid'. Verder ergert een paar mensen zich aan de anonimiteit waarin een aantal schrijvers zich hult. Onze favoriete abonnee ergert zich aan al onze excuses voor het onregelmatig verschijnen. 'Gewoon verschijnen als je een goed blad hebt. Niet eerder, niet later. Amen.

Wat kan er beter?

We vroegen wat er mist aan de Hack-Tic. 'Verschijningsfrequentie' riepen velen. Verder een hele lijst tips en suggesties. Te lang om hier op te noemen. Sommige suggesties zaten al in de planning voor volgende nummers, veel andere suggesties nemen we in overweging. Sommige mensen leveren zulke gedetailleerde suggesties dat ze het stuk zelf maar moeten schrijven!

Op de vraag wat er mist in Hack-Tic worden 'blote meiden' en 'tieten' opvallend vaak genoemd. In Hack-Tic 4 stond nog wel een naaktfoto (weliswaar van een telefooncel, maar toch..).

Conclusie

Of we er nu iets wijzer van zijn geworden? We weten het niet. Het begon als een poging om de nieuwgierigheid van een aantal redaktieleden te bevredigen, het ontaarde in een hels karwei om al die %@^#%$*formulieren in de computer in te voeren. Hieronder een voorbeeld om te laten zien door welke hel we zijn gegaan.

Het is duidelijk dat Hack-Tic lezers zich niet laten vangen in hokjes als links, rechts, arm of rijk. De resultaten liggen zo ver uit elkaar dat we zelfs niet echt van een gemiddelde lezer kunnen spreken. Het meest schokkende aan deze uitslag is daarom misschien wel dat de ware achtergronden van onze gemiddelde lezer een mysterie blijven.

Winnaar Demon-Dialer

Vanwege een communicatiefoutje stond er in het artikel bij de enquete dat er een Demon-Dialer te winnen was, terwijl we (nadat het artikel geschreven was) besloten om er een anonieme enquete van te maken. Stom natuurlijk. Veel mensen hadden ons door en hebben hun naam en adres er bijgezet voor het geval dat ... Dan zou het van ons wel erg lullig zijn om geen Demon te vergeven. De Demon gaat naar Jorge, student aan de UT in Enschede. In dit nummer verloten we maar even geen spullen, we zijn verdorie geen quiz!



The Hacker Crackdown

Een boekrecensie door Dave Barker-Plummer

Dave Barker-Plummer is als professor informatica verbonden aan het Swarthmore college in Pennsylvania. Hij doet onderzoek naar kunstmatige intelligentie en is mede oprichter van de Edinburgh Computers and Social Responsability discussion group. Zijn e-mail adres is plummer@cs.swarthmore.edu.

Bruce Sterling is cyberpunk science fiction auteur.

"The Hacker Crackdown: Law and Disorder on the Electronic Frontier", Bruce Sterling, Bantam Books, November 1992, ISBN 0-553-08058-X, 328 paginas.

"The Hacker Crackdown" is de term die Bruce Sterling gebruikt voor een serie inbeslagnames van computerapparatuur die plaatsvond in de zomer van 1990. De omstandigheden waarin deze invallen plaatsvonden, de mensen en gemeenschappen die ermee te maken kregen en de gevolgen voor de computergemeenschap en de samenleving als geheel, zijn het onderwerp van het boek.

Sterling, een cyberpunk-auteur, is als verhalenverteller op zijn best. Hij maakt gebruik van een onthullende schrijfstijl en is afwisselend verwonderd en geamuseerd als de loop der gebeurtenissen de ene vreemde wending na de andere neemt. Bijzonder intrigerend is zijn beschrijving van het Craig Neidorf/Knight Lightning verhaal. Neidorf werd vervolgd voor het electronisch verspreiden van een document dat zonder toestemming van een BellSouth computer was gekopieerd. Sterling documenteert de geschiedenis van dit document: het wordt meerdere malen over het Internet heen en weer wordt gestuurd en tenslotte gepubliceerd in Phrack. Neidorf wordt gearresteerd en het boek gaat over de aanklacht tegen hem, en tenslotte van het instorten van het proces. Als je dit leest realiseer je je dat de werkelijkheid nog een stuk vreemder is dan de cyberpunk fictie uit Sterling's andere boeken.

Er staan nog veel andere verhalen in het boek: het verhaal van Steve Jackson, wiens computerspellenbedrijf binnengevallen werd op grond van een verzegelde, dus niet direct bekendgemaakte, aanklacht. Alle computers werden in beslag genomen. Ook het verhaal van 'The Legion of Doom', een groep hackers die in cyberspace bij elkaar komen om op te scheppen over het inbreken in computers en om gestolen toegangscodes en creditcardnummers uit te wisselen. Het verhaal van de oprichting van de Electronic Frontier Foundation door Mitch Kapor, schrijver van Lotus 1-2-3 en John Perry Barlow, soms tekstschrijver voor de Grateful Dead. Aan het eind van het boek staat het verhaal van de Computer, Privacy and Freedom conference van 1992. Op deze conferentie konden hackers, politie, justitie en groepen die zich om bur-

gervrijheden bekommeren zeer open met elkaar praten.

Sterling probeert om over deze verhalen heen een beeld te scheppen van de cultuur, of beter gezegd, de culturen, van cyberspace. Hij kiest ervoor om zijn boek in vier stukken op te delen. Elk deel gaat over één van deze subculturen. Hacker-verhalen zijn al eerder verteld; Sterling verdient een pluim vanwege zijn poging om de achterliggende subculturen in beeld te brengen. Sterling lijkt echter niet op zijn gemak in zijn zelfbedachte positie als cultureel antropoloog. De gebeurtenissen blijven de personages overschaduwen, en het boek eindigt in verwarring. Maar uiteindelijk staat het hele onderwerp bol van verwarring: cultureel, technisch en ethisch.

Hoewel Sterling er niet genoeg nadruk op legt is `macht` het thema van het boek. In het eerste deel 'Crashing the System` beschrijft Sterling de macht van de telefoonmaatschappijen. Vanaf het begin van de techniek via de opkomst van AT&T en haar rol in regering en industrie naar het opbreken van AT&T in de Baby-Bells. Het beeld dat Sterling van de huidige telefoonmaatschappijen schetst is er een van een bedreigde machtsstructuur die vecht om haar greep op de macht, nu technologie steeds breder beschikbaar wordt en de economische monopolies gebroken worden. Als je denkt dat dit droog leesvoer is: er staat niet één zin in dit boek die je als `saai` zou kunnen omschrijven. Sterling brengt dit verhaal tot leven door te vertellen van telefonisten in het oude telefoonsysteem en de kids die het leuk vonden om zelf voor telefonist te spelen. Er zijn interessante parallelen tussen de tijd vlak na de uitvinding van de telefoon (de ontdekking van cyberspace) en de huidige tijd (het koloniseren van cyberspace).

In het tweede deel, 'The Digital Underground', komt de hacker subcultuur aan bod. Sterling blijft op een journalistiek middenpad: aan de ene kant benadrukt hij de illegaliteit van het hacken en ondermijnt hij de mythe van het getalenteerde genie, aan de andere kant legt hij er de nadruk op dat de hacker geen geharde crimineel is, maar meestal een 'kid'. Sterling legt het machtsgevoel uit dat een hacker voelt als hij een Voice Mail PBX of een ander beveiligd systeem kraakt; de hacker krijgt toegang tot tot dan toe afgesloten delen van cyberspace. Sterling beschrijft de isolatie en culturele onmacht van hackers. Het zijn over het algemeen jongens die zijn opgegroeid in het Reagan tijdperk en ze zijn gaan geloven dat alle instellingen corrupt zijn. Ze zien hun computer en modem als wapens tegen deze instellingen, al is het maar om onbelangrijke documenten te stelen, of zelfs alleen maar om te irriteren. Hij beschrijft ook het materiaal dat beschikbaar is op de underground bbs`en, om de anarchistische denkbeelden van deze groep aan te tonen. Volgens Sterling zijn er geen bendes hackers die samenwerken om de technocratie te ondermijnen, maar slechts eenlingen die het vanwege hun isolatie nodig hebben om tegen elkaar op te scheppen om een reputatie te krijgen, en die daarom vaak al snel worden gearresteerd. Isolatie is er ook voor verantwoordelijk dat bijna alle gearresteerde hackers volledig met justitie samenwerken. Er is geen hacker-gemeenschap, volgen Sterling, en ook geen hacker-eer.

In het derde deel, 'Law and Order', beschrijft Sterling de wereld van politie en justitie. Als er iets uit dit beeld naar voren komt, dan is het dat de Amerikaanse wetshandhavers slecht op het onderzoeken en vervolgen van computermisdaad zijn voorbereid. Sterling merkt op dat hij, een niet bijzonder computerminded auteur, meer computerpower in zijn huis heeft dan de gemiddelde computermisdaadbestrijder. Sterling beschrijft het mechanisme van een typische hacker inval; het inbeslag nemen van alles wat er technisch uitziet, inclusief CDs (waar immers data op zou kunnen staan) en Sony Walkmans. In zijn artikel 'Crime and Puzzlement' schrijft John Perry Barlow: "In alle eerlijkheid kan ik wel begrip opbrengen voor het probleem van de overheid. Dit is allemaal tamelijk magisch voor ze. Als ik de activiteiten van een heksenring stil wilde leggen zou ik waarschijnslijk ook alles meenemen dat ik tegenkwam. Hoe zou ik de keukenbezem van een ontsnappingsvoertuig kunnen onderscheiden?". Howel Sterling een sympathiek beeld schept van een overheid met te weinig geld, materiaal en kennis, probeert hij de excessen van 1990 niet goed te praten. Hij maakt een onderscheid tussen hackers en legitieme computergerbuikers, en hij beschrijft hoe beide groepen te lijden hebben gehad van de 'Hacker Crackdown'.

Tot slot beschrijft Sterling in het laatste deel, genaamd 'The Civil Libertarians', hoe de computergemeenschap reageerde op de vreemde gebeurtenissen van 1990 en hoe dit uitmondde in de oprichting van de Electronic Frontier Foundation. In dit optimistische deel beschrijft Sterling hoe de computerelite haar technische kennis gebruikte om te netwerken en te organiseren. Men kreeg de publieke opinie achter zich en vocht mee in de verdediging van Steve Jackson en Craig Neidorf. De EFF wierp zich op als verdediger van de grondrechten in cyberspace. In de ogen van de EFF was de 'Hacker Crackdown' de eerste veldslag om de controle over cyberspace. De 'Electronic Frontier' is een nieuwe 'plek' die op het moment gekoloniseerd wordt. De wetten van dit nieuwe gebied zijn op dit moment in de maak. De EFF vecht samen met anderen om de burgerrechten in dit gebied te verzekeren: vrijheid van meningsuiting, vrijheid van verzameling en privacy; een soort grondwet voor cyberspace.

'The Hacker Crackdown' heeft me veel geleerd over de gebeurtenissen in de vroege negentiger jaren en is afwisselend leuk en uitdagend. Ik raad het aan vanwege de discussie over macht en techniek, die geillustreerd wordt met ongelofelijke, maar ware, verhalen.

Unusual Facsimile Transmission Network

We kregen een fax van iemand die ons wilde aansluiten op het 'unusual fax transmission network'. Als je wilt meedoen hoef je alleen maar te faxen naar het nummer in het onderstaande symbool (in Engeland dus). Verder kost het niks, het net bestaat alleen maar om gekke dingen heen en weer te faxen. Wij hebben nog een fax met papier, dus hebben we ons maar niet aangesloten. Wel leuk als je je op je werk toch maar wat zit te vervelen!



Hacker als erkend dienstweigeraar

(Hannover/Keulen/Dresden) - "Computer-hacking" als levensovertuiging is een erkende reden om de dienstplicht te weigeren. Dit bevestigde het dienstweigeringshof van Dusseldorf tegenover de Keulse totaalweigeraar Jurgen Christ.

"Hacken is een bezigheid die noch criminele, noch commercieele achtergronden heeft. Informatie is een openbaar goed, dat gratis beschikbaar zou moeten zijn", aldus de 30-jarige journalist, die in de hack-scene als 'Bishop' door het leven gaat. De hacker-filosofie kent geen grenzen aan het recht op informatie, men noemt dit de 'free flow of information'. De geheimhoudingsstrategie van defensie, zowel in oorlogs- als in vredestijd, verhoudt zich slecht met dit streven.

Volgens het blad 'Datenschleuder' van de Chaos Computer Club heeft deze beslissing betrekking op iedereen die zich met open, vreedzame uitwisseling van informatie bezighoudt.

Duitse telefoonkaarten ook in Nederlandse cellen

(Bonn/Den Haag) - Vanaf 1994 zouden duitse telefoonkaarten ook moeten werken in nederlandse cellen, en vice versa. Dit volgens een persbericht van de Deutsche Telekom. De duitse cellen werken met chip-cards, de nederlandse met een optische rasterkaart. De firma Landis & Gear bouwt voor de PTT een zogenaamde 'allesslikker', een cel die optische kaarten, magneetkaarten en chipcards (franse en duitse) slikt. Ook de telecards van beide PTTs zouden over de grens moeten gaan functioneren. De nederlandse Telecard is een magneetkaart die met een credit-card te vergelijken is.

Hack-Tic ook dit jaar op de HCC beurs

Op vrijdag 20 november en zaterdag 21 november is Hack-Tic weer heftig aanwezig op de HCC beurs in de jaarbeurshallen in Utrecht. Op stand K71 staan we met Hack-Tics (alle oude nummers voorradig), Demon-Dialers, een demonstratie van het Hack-Tic Netwerk en nog veel meer. Op deze pagina een bon die 2.50 korting geeft op de toegangsprijs. Als je deze Hack-Tic heel wilt houden mag je hem ook kopieeren. Pas Op: Als je meer dan 1 kopie maakt zal deze Hack-Tic exploderen.



Wet van Murphy

Uitgeverij Lannoo brengt het boek 'De Computerwetten van Murphy' van Joachim Graf. Want, zo schrijven ze: "Geen enkel onderzoek heeft meer bijgedragen tot het begrijpen van onze industrieele samenleving en de informatiemaatschappij dan de wet van Murphy. Wie voor ogen houdt dat alles wat mis kan gaan onherroepelijk mis zal gaan, wordt doordrongen van een diep inzicht in de wereld, in het leven op zichzelf en in heel de rest."

Pogingen om de computers een zekere mate van intelligentie mee te geven zijn volgens de uitgever fataal mislukt, maar achterbaksheid, geniepigheid en sluwheid zijn al optimaal ontwikkeld.

Chipcard in India

Sommigen denken dat onze maatschappij technisch op een hoog niveau staat. Wat blijkt: in India hebben ze al weer enige tijd chipcards voor de telefooncellen.



CCC'92

Dit jaar is het Chaos Congres net als vorig jaar van 27 t/m 29 december in het Eidelstatter Burgerhaus in Hamburg. De Hack-Tic redaktie is zoals elk jaar aanwezig. Maar je kunt ons natuurlijk ook op de HCC-beurs opzoeken.